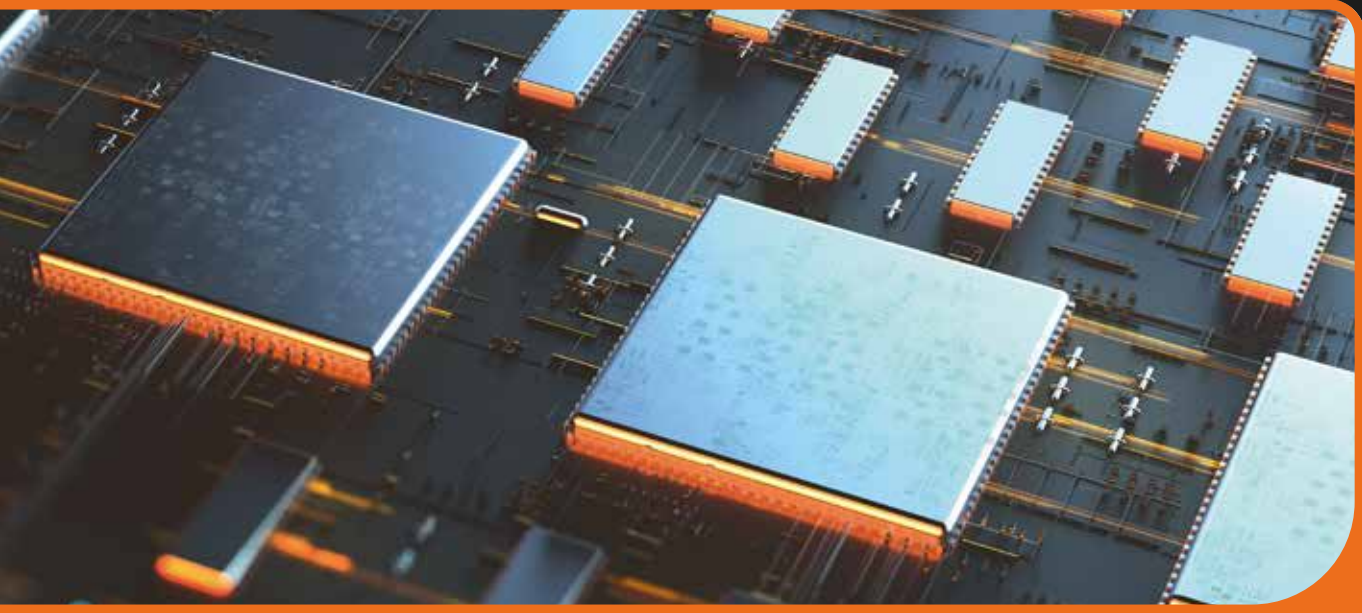
International
Comparative
Legal Guides



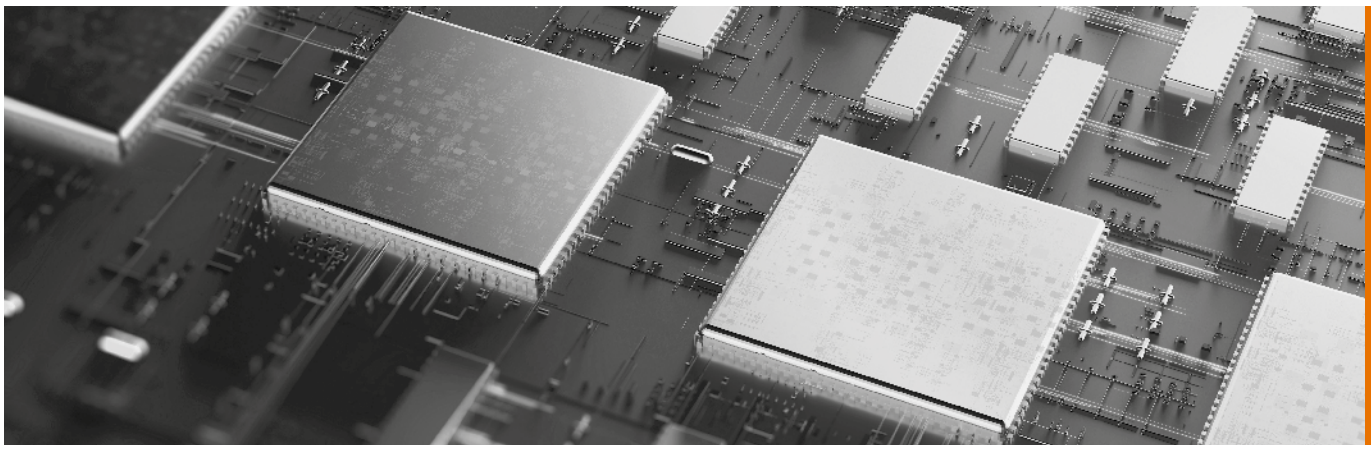
Practical cross-border insights into cybersecurity

Cybersecurity 2022

Fifth Edition

Contributing Editor:
Nigel Parker
Allen & Overy LLP

ICLG.com



ISBN 978-1-83918-152-8
ISSN 2515-4206

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Publisher
James Strode

Production Editor
Jenna Feasey

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

International Comparative Legal Guides

Cybersecurity 2022

Fifth Edition

Contributing Editor:
Nigel Parker
Allen & Overy LLP

Expert Analysis Chapters

Q&A Chapters

From the Publisher

Dear Reader,

Welcome to the fifth edition of *ICLG – Cybersecurity*, published by Global Legal Group.

This publication provides corporate counsel and international practitioners with comprehensive jurisdiction-by-jurisdiction guidance to cybersecurity laws and regulations around the world, and is also available at www.iclg.com.

This year, four expert chapters provide insight into ransomware, directors' liabilities, cybersecurity and international sanctions, and the use of AI.

The question and answer chapters, which in this edition cover 23 jurisdictions, provide detailed answers to common questions raised by professionals dealing with cybersecurity laws and regulations.

As always, this publication has been written by leading cybersecurity lawyers and industry specialists, for whose invaluable contributions the editors and publishers are extremely grateful.

Global Legal Group would also like to extend special thanks to contributing editor Nigel Parker of Allen & Overy LLP for his leadership, support and expertise in bringing this project to fruition.

James Strode
Publisher
Global Legal Group

ICLG.com

Infiltrate, Extort, Repeat – The Ransomware Pandemic


Nigel Parker


Nathan Charnock


Daniel Ruben

Allen & Overy LLP

Introduction

The last two years have seen a pandemic of epic proportions sweep across the globe, wreaking havoc in its wake and doing untold damage to the lives of billions. As organisations have adapted to deal with unprecedented challenges posed by COVID-19, hackers have taken advantage of a febrile environment, resulting in a spike in so-called "ransomware" attacks. These have had a sometimes-crippling effect on countless organisations, large and small. Often, victims must decide between paying a ransom, to restore systems and recover data, or refusing and facing potentially significant costs and catastrophic business interruption.

In this chapter we explore some of the strategies that can be implemented to prepare for, and minimise the impact of, a ransomware attack. We also consider the merits, legality and practicalities of paying a ransom.

Ransomware on the Rise

Ransomware is a form of malware that, once infecting a computer or system, encrypts data and files to render them inaccessible and unusable. Attackers will then typically send a ransom note demanding payment in return for the decryption keys required to restore access, and may threaten to publicly release sensitive data that they have obtained during the attack as a form of "double extortion".

Ransomware attacks pose a growing risk as they become more lucrative and easier to carry out. The emergence of groups offering so-called "Ransomware-as-a-Service" (RaaS), such as REvil and DarkSide, combined with the ready availability of on-demand malware kits, has made the process simpler than ever for would-be attackers. In addition, hackers typically demand payment in anonymous cryptocurrency that is difficult to trace, further reducing the risk of repercussions.

The COVID-19 pandemic fundamentally changed the way many access their online systems, with remote access systems such as remote desktop protocol (RDP) servers and virtual private networks (VPNs) becoming fundamental to the operation of businesses worldwide, as people logged on from home. This extension of networks gave rise to new vulnerabilities for exploitation by hackers using a combination of weak passwords, credentials gained through phishing attacks, the absence of multi-factor authentication and software deficiencies. The result – an estimated 300 million ransomware attacks were carried out in 2020, a rise of more than 150% on the prior year.[1]

In 2021, business costs associated with ransomware were expected to hit $20 billion, while cyber insurers have reported a fourfold jump in claims from 2019 through 2020.[2] This rise in costs is being driven in part by the "big game hunting" tactic that is being adopted by many attackers. Larger companies have been targeted with the aim of extracting larger ransoms, driven by the knowledge that many will not be able to endure the damage resulting from the average 15 business days of downtime caused by ransomware attacks.[3] In March 2021, we saw US insurance giant CNA Financial pay $40 million to regain control of its network;[4] in the same month, Acer received what is thought to be the largest ransom demand to date when REvil offered a "discounted rate" of $50 million while using stolen corporate data from the electronics manufacturer as leverage.[5] According to Palo Alto Networks, the average ransomware payment increased by 171% to $312,493 in 2020.

Fortify Your Defences and Equip Your Team

As with all forms of cyber-attack, it is a huge challenge to prevent ransomware attacks from occurring. The continuous nature of technological change, software development, and support and maintenance, combined with growing sophistication and frequency of attacks, means that even the most proficient of information security teams can struggle to stay one step ahead of the attackers. What businesses can do is ensure they invest in information security as a key priority and have robust programmes and procedures in place to ensure they are well prepared in the event that they become a target of attackers. The UK's National Cyber Security Centre recommends adopting a "defence-in-depth" approach, constructing multiple layers of defences with mitigations at each layer to best improve the opportunity to identify potential ransomware attacks and address them before they are able to cause damage.[6]

As a minimum, businesses should ensure they have:

1. **A well-resourced security programme**: A comprehensive information security programme is perhaps the most effective way businesses can reduce the risk that they fall victim to a ransomware attack. The scope of these programmes can be vast depending on the size and complexity of technology

stacks. However, a baseline programme for all medium-large businesses should include the implementation of appropriate antivirus and anti-malware software, regular and proactive network monitoring (on a 24/7/365 basis), regular patching and software updates, robust access controls including the use of multi-factor authentication and other human verification systems (for all remote access points) and use of other network-based bot management tools to detect illegitimate traffic.

2. **Appropriate internal training**: Many attacks are caused by human error or inaction. It is imperative that all staff receive regular training so they are aware of the risks associated with cyber-attacks and understand their own role in preventing and responding to them. Phishing was the second most common cause of ransomware attacks identified by Group-IB,[7] and providing simple tips to help employees recognise malicious emails can help reduce the risk of a successful attack.
3. **Incident response plans and procedures**: Organisations should ensure that they have detailed incident response procedures in place and should conduct regular table-top exercises to test these procedures and ensure relevant personnel (including senior personnel) understand their roles. The response procedures should include a predefined list of critical systems of which recovery is to be prioritised.
4. **Business continuity plan and disaster recovery**: In addition to general business continuity and disaster recovery plans, organisations should design a strategy for recovering in the event of a ransomware attack to minimise disruption and allow for continued operation of key business functions while remedying any attack suffered. Incident response procedures should be tested under disaster recovery conditions to ensure that they are workable in such scenarios. Often ransomware attacks can restrict the use of email and business mobile phones; therefore having a plan that enables core teams to work without these functions is imperative.
5. **Maintain regular back-ups**: Regularly backing up data and ensuring that these back-ups are secured is vital to preparing for any potential ransomware attacks. Having access to back-ups of important files, stored in multiple locations both locally and on cloud-based services, which are separate from and not connected to the network, will allow access to these files to be maintained in the event of an attack. Sophos found that 56% of victims of ransomware attacks in 2020 were able to use back-ups to retrieve their data, rather than paying a ransom.[8]
6. **Internal expertise**: A well-resourced team of information security specialists is essential to enable a business to maintain its day-to-day operations, to manage and implement its security programme and to react in the event of an incident.
7. **Access to external resource and expertise**: When an attack occurs, a business will likely want to engage external support from external specialists, including those with expertise in incident response, dark web monitoring, system rebuild, cyber forensics and PR management as well as external legal counsel who can assist with regulatory notifications, complaints, enforcement against third parties and advising on the payment of ransoms. Establishing these relationships (and putting in place engagement terms) before an attack has occurred will save a huge amount of time in the vital hours immediately following an incident.
8. **Accountability and risk monitoring**: The appointment of a Chief Information Security Officer or another senior executive officer with responsibility and accountability for information security (as well as appropriate incentives) will drive good performance and ensure that senior executives are alive to and aware of the risks associated with ransomware attacks.

React, Respond and Remediate

Each ransomware attack will present a unique set of circumstances, but as part of your incident response process you should ensure you:

1. **Triage** – conduct an initial triage of the incident as quickly as possible so you can establish the facts and better understand the scope and impact of the attacks and assess its severity.
2. **Instigate incident management procedures** – involve key stakeholders such as representatives from the information security, IT and legal teams as well as communications and customer service representatives where relevant. It is important to keep detailed incident logs to record decisions and to use out-of-band modes of communication such as telephone calls to avoid tipping off the attackers or any other malicious surveillance.
3. **Implement initial remediation steps as soon as possible** to try to stop the attack or at least prevent further spread of the malware across multiple systems and servers. Implement disaster recovery and business continuity plans and look to contain the incident and evaluate whether there is a risk of the attackers moving across other servers that are yet to be affected, whether locally or globally. This may involve quickly isolating or disconnecting affected systems and resetting credentials and passwords (including compromised admin credentials). Following the initial response, work will likely need to begin to clean the infected devices and reinstall the operating system (prioritising key systems first). The team must then ensure that both the cleaned devices/systems and the back-ups are free from any ransomware before restoring data from the back-up and reconnecting systems to a clean network. Of course, if a ransom is paid and data is released, the business may be able to avoid a full-scale rebuild.
4. **Brief senior executives** of events to ensure they are up to speed and able to take important decisions quickly (including whether to pay a ransom and dealing with any media interest).
5. **Deploy third-party advisors** to assist with your response. As noted above, these could range from specialists in incident response, dark web monitoring, system rebuild, cyber forensics and PR management as well as external legal counsel who can assist with the regulatory response. These specialists may also be able to help you to contact and negotiate with the attackers.
6. **Work with other interested third parties** who may have had corporate or other sensitive data compromised or accessed during the attack. Consider liaising with financial service providers to help prevent fraudulent activity if customer information has been accessed.
7. **Consider involving law enforcement** who may be able to assist with the investigation and help facilitate any ransom payments. You will want to take local legal advice here depending on the jurisdiction involved.
8. **Make regulatory and contractual notifications** where required, including to data protection authorities or other industry or government regulators. These often need to be made within a very short period of time. The business may also have contractual obligations to notify third parties of the breach.

9. **Complete a detailed incident review** to analyse how the ransomware attack was able to succeed, how the organisation responded and what lessons could be learned. Set a deadline and ensure accountability for implementation of any identified remediation measures.

The Hostage Dilemma – Should You Pay the Ransom?

A ransomware attack has spread across your key business systems and the attackers have access to huge volumes of sensitive customer, commercial and employee data. Thankfully you have good back-ups in place but rebuilding and restoring your systems will take weeks and the attackers are threatening to release that sensitive information on the dark web, unless you pay them $5 million in Bitcoin. What do you do?

This question raises a number of issues for businesses, including ethical dilemmas, practical and operational difficulties, legal complications, financial challenges and public relations headaches. In all cases, the decision to pay a ransom needs to be taken carefully, with a very small group of senior stakeholders and the input of external advisors where appropriate.

The initial answer is usually: "No – we will not negotiate with the attackers." However, many businesses do often decide that ransoms are a price worth paying when faced with the alternative of an unknown period of business disruption, potentially combined with the prospect of sensitive data either being leaked or irretrievably lost.

Richard Hanlon of Aon Cyber Solutions thinks that "paying the ransom is the tip of the iceberg" and that "whatever the business, it's better to understand ransomware losses in the context of business interruption, because that's the single biggest threat from a ransomware attack". The UK's National Health Service incurred £92 million of costs to restore its services in the months following the 2017 WannaCry attack. It is also important to note that losses can extend well beyond remediation expenses, as victims may find themselves exposed to long-term impacts such as loss of business, third-party claims and reputational damage. Research by Sophos estimated that, last year, the average cost of rectifying a ransomware attack, when considering downtime and the costs associated with recovery, sat at $1.85 million with 26% of victims choosing to pay ransoms.[9] In the first part of 2021, this figure had risen to 32%.[10]

Whilst the payment of a ransom may ultimately be a commercial decision, there are a number of other considerations that a business will want to take into account when choosing whether or not to pay:

- **Attacker credibility/reliability**: If cyber specialists are able to identify the likely attacker, it will be helpful for your business to understand whether that particular attacker/group has a reputation for ceasing an attack and returning stolen data when they receive a ransom payment.
- **Governmental and societal pressures**: Depending on the nature of the business and the jurisdictions impacted, victims may want to consider what view government bodies may take of paying a ransom. Experts within the cybersecurity industry remain deeply divided on whether victims should pay ransoms. The Ransomware Task Force, a global coalition of cyber experts, has made nearly 50 recommendations to governments across the world to help curb the burgeoning illicit industry but were unable to come to an agreement on whether countries should ban ransom payments. In the United States, the FBI does not advocate the paying of ransoms, in part because it does not guarantee that access will be regained, while in the last year the US Department of the Treasury's Office of Foreign Assets Control has looked to impose financial penalties on organisations that make ransomware payments and in doing so "may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims".
- **Legal restrictions**: It will also be important to consider if there are any legal restrictions that prevent or restrict the payment of ransoms in the affected jurisdictions. For example, in the UK, whilst the payment of ransoms is not illegal in most situations, there is a risk that making such a payment could be considered a criminal offence under the Terrorism Act 2000 if it is known or there is reasonable cause to expect that the person receiving the payment will or may use it for the purposes of funding terrorism.
- **Ethical stance**: Many businesses will also want to consider their own moral stance on paying a ransom. These payments typically involving the funding of a criminal enterprise that is likely to repeat the offence elsewhere and funnel the funds into further illegal activities. This reality will have to be weighed against the costs of any potential harm that may arise from the attack continuing, such as the release of huge amounts of sensitive data. Increasingly, organisations are implementing policies that set out their position on the payment of ransoms in different circumstances.
- **Reputational risk**: Whilst many businesses will try to keep details of any ransom payment confined to a small number of senior individuals, there remains a risk of a leak. Therefore, careful consideration of the public relations impact will need to be considered and a communications plan implemented.
- **Financial impact**: Businesses should take a holistic view of the financial impact of paying a ransom, considering not just the payment itself but also the cost of the attack continuing and the impact of the attack of revenues generally (whether or not a ransom is paid).
- **Practicalities**: Importantly, if a business does decide to make a ransom payment, there are a number of practicalities to consider. In particular, access to cryptocurrency will be needed in short order and an organisation will need to decide who will need to sign off on and make the relevant payment. In addition, depending on the jurisdiction, businesses may also want to inform law enforcement of an intention to make the payment to ensure transparency and to enable them to provide any assistance.

Conclusion

The COVID-19 pandemic provided a breeding ground for cyber criminals to infiltrate organisations on a scale not seen before, with ransomware the malware of choice for many seeking to cause maximum disruption to businesses during already challenging times. The ethics of paying a ransom still divide opinion across the world but the devastating effects of not doing so means businesses face a very real dilemma when making this tough decision. The most effective way to address the threat of these attacks is to invest in strong defences and experienced personnel whilst implementing robust processes and procedures so that a business stands ready to react, respond and remediate any incidents that occur.

Endnotes

1. *Help Net Security*, "Number of ransomware attacks grew by more than 150%", 8 March 2021.
2. *The One Brief*, "It's Time to Forget These 5 Ransomware Myths", 14 July 2021.
3. *Health IT Security*, "Ransomware Causes 15 Days of EHR Downtime, as Payments Avg $111k", 4 May 2020.
4. *Bloomberg*, "CNA Financial Paid $40 Million in Ransom After March Cyberattack", 20 May 2021.
5. *Forbes*, "Acer Faced With Ransom Up To $100 Million After Hackers Breach Network", 21 March 2021.
6. *National Cyber Security Centre*, "Mitigating malware and ransomware attacks", 9 September 2021.
7. *Ibid.*, endnote 1.
8. *Sophos*, "The State of Ransomware 2021" A Sophos Whitepaper, April 2021.
9. *Ibid.*, endnote 8.
10. *Ibid.*, endnote 8.

Nigel Parker is a partner specialising in intellectual property, data protection and privacy, commercial contracts and IT law. He is a member of the firm's Cyber Security Group and has advised clients on strategies for managing legal risk in relation to cybersecurity, including the deployment of a variety of risk management tools, on the response to attacks and dealing with regulatory authorities, and on taking pro-active steps in response to attacks.
Nigel is recognised in *Chambers* and *The Legal 500*. He was named one of the "Top 40 under 40" data lawyers by *Global Data Review*.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 3136
Email: nigel.parker@allenovery.com
URL: www.allenovery.com

Nathan Charnock is an associate specialising in commercial contracts, data protection and privacy, intellectual property and IT law. He advises clients on their response to cybersecurity attacks, including their interactions with regulators and implementation of remediation steps. Nathan also advises on complex commercial arrangements for a range of clients in the technology, retail, telecommunication, life sciences and financial services sectors, including IP licensing, outsourcing and service provision arrangements.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 3899
Email: nathan.charnock@allenovery.com
URL: www.allenovery.com

Daniel Ruben is a trainee solicitor in the commercial team at Allen & Overy.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

URL: www.allenovery.com

Allen & Overy is a full-service global elite law firm headquartered in London. Our commitment to help our clients deliver their global strategies has seen us build a truly global network now spanning over 40 offices. We have also developed strong ties with relationship law firms in more than 100 countries where we do not have a presence.
We have a strong cybersecurity practice comprising a core team of 19 partners with diverse backgrounds in data protection, bank regulation, anti-trust, securities laws, technology, IT, litigation, employment, IP and corporate. This spread is crucial because cybersecurity Incidents frequently span a wide range of traditional legal practice areas. There is an important legal component to cybersecurity and our integrated team of diverse practitioners reflects this requirement. As a full-service global elite law firm, we are able to advise clients on all legal issues concerning cybersecurity.

www.allenovery.com

ALLEN & OVERY

Phantom Responsibility: How Data Security and Privacy Lapses Can Lead to Personal Liability for Officers and Directors

Rothwell Figg

Christopher Ott

2021 has made it clear: boards of directors ignore data security and privacy risks to companies at the peril of their companies and – increasingly – their own personal liability. A business has its operations halted by ransomware approximately every 10 seconds. Just in this last year, a United States oil pipeline was shut down by these cybersecurity threats. The global costs of these breaches and online crime exceeds trillions of dollars every year. These potential costs have elevated data security and privacy issues from mere "IT issues" to the centrepiece of strategic risk management. As a result, boards face expanding personal legal liability for the company's data security and privacy failures.

The upward liability trend is not new. As early as 2014, the National Association of Corporate Directors (NACD) Director's Handbook on Cyber-Risk Oversight provided core cybersecurity principles to members of public companies, private companies, and non-profit organisations of all sizes and in every industry sector. The NACD directed board members to understand and approach cybersecurity as an enterprise-wide risk management issue and not just an issue for the IT team. As an established enterprise-wide risk, cybersecurity therefore began triggering boards' existing legal obligations. In the same year as the NACD handbook's admonition, 2014, SEC (Securities and Exchange Commission) Commissioner Luis Aquilar stated that "boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility do so at their own peril". The new regulators at the SEC, led by Director of Enforcement, Gurbir Grewal, have taken an even more aggressive stance in the last year.

Those perils are changing in real time, just as cybersecurity and privacy threats are changing. However, we can identify certain concrete areas of established liability and strategically identify the emergent risks. Right now, the main liability risks to boards include:

- SEC liability for cyber risks;
- SEC liability for privacy risks;
- officers' and directors' civil liability for breached fiduciary duties;
- direct liability for violation of state data security and privacy statutes, with a special emphasis on California;
- criminal liability for cybersecurity and privacy failures; and
- global civil and regulatory liability, with a special focus on the New York Department of Financial Services (NYDFS) and EU Regulations.

In this chapter, we attempt to explore all of these current trends. At the very end, we will also tackle a few harder-to-classify risks related to United States national security oversight of cyber readiness.

United States: Officers' and Directors' Personal Liability for Cybersecurity and Privacy Failures

On February 21, 2018, the SEC "voted unanimously to approve a statement and interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents".[1] The SEC did not wait long for the public to absorb this guidance. On April 24, 2018, the SEC "announced that the entity formerly known as Yahoo! Inc. has agreed to pay a $35 million penalty to settle charges that it misled investors by failing to disclose one of the world's largest data breaches in which hackers stole personal data relating to hundreds of millions of user accounts".[2] In the space of two months, the SEC went from "companies also may have disclosure obligations" for breaches to paying $35 million for failure to disclose.[3] When the expectations change so quickly, it is important for officers and directors to understand both the current and developing state of cyber and privacy risks, especially when it comes to personal liability.

SEC liability

The SEC maintains broad (and expanding) authority over directors. This authority begins the moment that a director is named. SEC proxy disclosure rules, among other requirements, mandate that companies disclose, for each director and nominee, the specific experience, qualifications, attributes or skills that led to the conclusion that the individual should serve as a director of the company in light of its business and structure.[4] This disclosure must be made on an individual basis and be specifically linked to the biographical description of each director and nominee. These new disclosure requirements theoretically expose directors to greater potential liability if they are identified in an SEC filing as having a particularly valuable skill or expertise that is valued and relied upon by the company.

The pitfalls of director "cyber hype"

Directors and their companies often tout directors' particular skills that they bring to the board. It makes sense, therefore, that a director may tout their particular cybersecurity *bona fides*. However, overselling one's cyber skills can bring individual liability. In 2003, the SEC amended the proxy disclosure rules to require that a company disclose whether it has at least one "audit committee financial expert" on its audit committee.[5] Prior rules indicated that identifying a director as an expert did not increase their liability for registration statements pursuant to Section 11 of the Securities Act of 1933 (Securities Act), dealing with

liability in connection with registration statements. The safe harbour covered more than merely directors' financial expertise. However, the entire safe harbour language was removed in the wake of the Sarbanes-Oxley Act. Therefore, real individual liability risks flow from whenever a board member touts their expertise in any field, including cybersecurity and privacy.

Section 11 of the Securities Act imposes civil liability on directors of an issuer if "any part of the registration statement, when such part became effective, contained an untrue statement of a material fact or omitted to state a material fact required to be stated therein or necessary to make the statements therein not misleading". Therefore, directors face a real dilemma in that they feel that they should tout their material skills to current and potential shareholders but responsibility and liability flow from those representations. Fortunately, there are many defences available to directors that turn on their level of knowledge.[6] These same defences could be utilised to defend against a Section 11 claim levelled against a director.

Overstatements of cyber readiness now regularly result in SEC liability. For example, in August 2021, the SEC announced a $1million fine against a London-based public company that allegedly misled investors about a 2018 cyber intrusion involving the theft of millions of student records.[7] To avoid a similar outcome:

1. avoid making subjective public statements about an organisation's cybersecurity or data privacy (e.g., the company has "strict" protections in place). These types of statement are very difficult to affirmatively prove as "true";
2. do not describe information as a "potential" risk, if you know that the risk has become reality. For example, it is impermissible to report that a breach "may" include dates of births, where the organisation knows it did;
3. implement a formal process for timely identifying and patching known vulnerabilities (e.g., the company allegedly failed to patch a critical vulnerability for six months after it had been notified); and
4. design disclosure controls and procedures to ensure that those responsible for making disclosure determinations are adequately and timely informed before making and approving public statements. These procedures can and should include:
    a. Initial Investigation:
        i. steps to identify and investigate cybersecurity incidents;
        ii. a plan to automatically assess and analyse the impact of the incident on the company's business and customers;
        iii. a plan to automatically ensure careful analysis of whether the cybersecurity incident is material, giving rise to disclosure obligations;
        iv. a plan to automatically refer potentially material cybersecurity incidents to appropriate committees, including the disclosure committee, for assessment and analysis;
        v. a plan to automatically ensure that material cybersecurity incidents are reported to senior management and to the board of directors; and
        vi. a plan to automatically ensure that material cybersecurity incidents are disclosed to investors and that existing disclosures are reviewed and, if necessary, updated if new facts render them incorrect or misleading.
    b. Mitigation and Remediation:
        i. steps and deadlines to remediate incidents based on severity;
        ii. expressly stating the circumstances under which trading restrictions should be imposed on company personnel who are in possession of material non-public information (MNPI) regarding the incident; and
        iii. provide for the issuance of a document preservation or litigation hold for material incidents or other incidents where the company anticipates litigation.

Board cybersecurity and privacy risk oversight

Item 407(h) of Regulation S-K and Item 7 of Schedule 14A require a company to disclose the extent of its board of directors' role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board's leadership structure.[8] The SEC has previously said that "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company".[9] The SEC has expressly stated that cybersecurity risks are among those that must be reported to directors, with all of the criminal and civil liability that may flow from that notice.[10]

In addition to the cybersecurity actions just discussed, the SEC has also imposed liability upon executive directors for privacy failures. In September 2021, the SEC hit "alternative data provider" App Annie with a $10 million fine and its CEO with a $300,000 fine.[11] Among other failures, the SEC alleges that App Annie misrepresented to users how it would use their data, which constitutes a privacy violation, not a cybersecurity lapse. Specifically, App Annie told customers that it would only use their data in an "aggregated and anonymized form", when it also used such data in a "non-aggregated and non-anonymized form". This misrepresentation, which was obviously fairly technical, resulted in a personal fine upon the CEO. For this reason, officers and directors must take pains to avoid overstating what your company is doing with respect to security or privacy. This includes even these technical aggregation characterisations. If your company does not fully anonymise data or only uses data in an aggregated form, take care to describe your actual uses. Also, officers and directors need to be aware if the company makes a material change in its approach to handling data privacy. Companies must build mechanisms that will alert users to these changes with a clear notice. The SEC has since begun enforcing these requirements with gusto. Of particular note, the SEC has concluded that merely having a policy is insufficient.

On August 30, 2021, the SEC announced the sanctions of eight firms in three actions for alleged "failures in their cybersecurity policies and procedures that resulted in email account takeovers exposing the personal information of thousands of customers and clients at each firm".[12] These actions all also alleged violations of the "Safeguards Rule", Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)), which is designed to ensure that investment advisers and broker-dealers protect confidential customer information. All were SEC-registered as broker dealers, investment advisory firms, or both. The SEC Enforcement Division's Cyber Unit noted that "[i]t is not enough to write a policy requiring enhanced security measures if those requirements are not implemented or are only partially implemented, especially in the face of known attacks".

According to the SEC's order against the Cetera entities, between November 2017 and June 2020, cloud-based email accounts of over 60 Cetera Entities' personnel were taken over by unauthorised third parties, resulting in the exposure of personally identifying information of at least 4,388 customers and clients. Cetera protected none of the affected accounts consistent with their own policies. The SEC's order also finds that Cetera sent breach notifications to the firms' clients that included misleading language regarding the promptness of the notifications after discovery of the breach.

According to the SEC's order against Cambridge, between January 2018 and July 2021, cloud-based email accounts of over 121 Cambridge representatives were taken over by unauthorised third parties, resulting in the PII exposure of at least 2,177 Cambridge customers and clients. The SEC's order concluded that Cambridge, despite notice of breaches in 2018, failed to adopt and implement firm-wide enhanced security measures for cloud-based email accounts of its representatives until 2021, resulting in the exposure and potential exposure of additional customer and client records and information.

According to the SEC's order against KMS Financial Services (KMS), between September 2018 and December 2019, unauthorised third parties hijacked cloud-based email accounts of 15 KMS financial advisers or their assistants, resulting in the data exposure of approximately 4,900 KMS customers and clients. KMS failed to adopt written policies and procedures requiring additional firm-wide security measures until May 2020, and did not fully implement those additional security measures firm-wide until August 2020, placing additional customer and client records and information at risk.

Cybersecurity risks and scrutiny of board trading activities

Directors also will face scrutiny for their trades after they are advised of cybersecurity risks. In the wrong situation, a trade could be considered to be an insider trade on non-public information. There is a delicate balance that must be reached here. After all, directors should righteously be informed of significant risks, such as cybersecurity or accounting matters. However, directors must internalise that their cybersecurity briefings can be every bit as material as their regular briefings on accounting controls or other vintage risks. Currently, however, director understanding may be lagging behind their responsibilities.

In the massive Equifax breach, multiple insiders have been charged for trading on the breach information.[13] The SEC has signalled that it will make this type of trading a particular focus.[14] For this reason, the SEC advises that "[c]ompanies should assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications and to facilitate policies and procedures designed to prohibit directors, officers, and other corporate insiders from trading on the basis of material nonpublic information about cybersecurity risks and incidents".[15] That may be easier said than done.

As a practical matter, companies can start to protect their officers and directors from this type of scrutiny (and prevent the underlying suspect behaviour) by establishing policies and procedures in place that:

1. provide regular training to all insiders about cybersecurity risks must be treated like any other material enterprise risks and ensure that the company makes quick and timely disclosure of any material non-public cybersecurity information; and
2. expressly address trading blackouts or similar procedures that will prevent directors, officers, and other corporate insiders from trading during the heightened period between the company's discovery of a cybersecurity incident and public disclosure of the incident to trade on MNPI about the incident.

Other United States Federal Regulators

This year, the Financial Industry Regulatory Authority (FINRA) issued a lengthy "notice" to "remind member firms of their obligation to establish and maintain a supervisory system, including written supervisory procedures, for any activities or functions performed by third-party vendors, including any sub-vendors that are reasonably designed to achieve compliance with applicable securities laws and regulations and with applicable FINRA rules".[16]

The notice "reiterates applicable regulatory obligations; summarises recent trends in examination findings, observations and disciplinary actions; and provides questions member firms may consider when evaluating their systems, procedures and controls relating to Vendor management".

The FINRA also notes that the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency recently published and requested comment on proposed guidance designed to help banking organisations manage risks associated with third-party relationships.[17]

There are also additional risks from unfamiliar regulatory arms. As part of its reckoning with ransomware events, the United States is turning to sanctions remedies. The Office of Foreign Assets Control (OFAC) is an arm of the U.S. Treasury Department that administers and enforces economic and trade. The OFAC is therefore now administering sanctions in pursuit of private companies' cybersecurity objectives. This may be a necessary step but the intersection of sanctions penalties and private cybersecurity has the potential to be messy. Among other things, this raises the possibility that merely paying the ransomware demand may violate United States laws. A fraught situation has potentially become even more complicated.

Officer and director fiduciary duty law and personal civil liability

Officers and directors can face civil liability if they breach their fiduciary duties, which can lead to a shareholder derivative action wherein the shareholders sue the officers and directors for breaches that harmed the company. Technically, every state has its own standards regarding the fiduciary duties that officers and directors owe to companies and, by extension, the shareholders. Because so many companies are incorporated there, Delaware generally leads the way of fiduciary duty issues. Under Delaware law, directors owe fiduciary duties of care and loyalty to the company.[18] This fiduciary duty of care requires directors to act with a degree of care that ordinary careful and prudent men would use in similar circumstances.[19] Under this standard, directors must act on an informed basis, in good faith, and in the honest belief that the action was in the best interests of the company.[20] Courts have interpreted that this duty of loyalty further includes a duty of oversight, which will be breached if directors "utterly fail" to implement any reporting or information systems or controls or if, after implementing these systems, directors fail to monitor or oversee the operation of these plans.[21] Therefore, Delaware law clearly establishes that officers and directors must set up informational and reporting systems and monitor the results of those systems.

It does not take much imagination to see how these standards could be applied to the new information technology and cybersecurity systems that boards oversee in various companies. A number of derivative actions have been filed following high-profile data breaches. These actions are typically based on claims that, by failing to implement adequate information security policies, the directors allowed a breach to occur that damaged shareholders through decreased stock prices. Although claimants in these cases face a high pleading standard, which we will discuss below, the cases remain expensive and disruptive. Indeed, they can often to lead to resignations by officers and directors.

Civil liability for false and misleading public cybersecurity statements

Companies' public cybersecurity statements or even certain kinds of silence can also create officer and director liability. Section 10(b) and Rule 10b-5 of the Exchange Act prohibit, *inter alia*, making untrue or misleading statements of material fact. These laws further prohibit selective silence about these material facts. Therefore, omitting material facts must not be left unstated if they are necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading. This last requirement is a mouthful. However, in more accessible language: one must tell the truth about anything that is important to the company and one must volunteer facts wherever silence on those facts will actually mislead someone. These requirements to be truthful and forthcoming with the public could conceivably create significant officer and director cyber liability in civil class actions. However, this type of liability will not attach merely when someone wishes to second-guess the content and omissions of companies' cybersecurity statements. As with many liability issues, the quantum of one's knowledge matters.

Unlike Section 11 of the Securities Act discussed earlier, when it comes to exaggerating directors' cybersecurity skills, Section 10(b) requires the intent to deceive, manipulate or defraud, otherwise known as "scienter". Without proof that the director acted with that corrupt scienter, there can be no Section 10(b) liability. That proof of scienter will be absent for many, although not all, officers and directors.

Expert experience and director liability

Experience and context matter when it comes to scienter. Directors with a particular technical or cybersecurity expertise may have difficulty getting Rule 10b-5 claims dismissed because it may be easier for plaintiffs to plead scienter as to them. The *In re U.S. Bioscience Securities Litigation*[22] involved a class action by purchasers of a company's stock against the directors. The judge denied a motion to dismiss Section 10(b) claims against certain outside directors of the company for alleged misstatements, contained in the annual Form 10-K, suggesting that one of the company's products was more effective and further along in clinical trials than was warranted by the facts. In rejecting the motion, the judge explained that "[o]utside directors can be of two very different kinds", those whose role is not intended to be hands on and those who have valuable expertise in the industry.[23] In that case, the directors' "valuable expertise in [the company's] industry" made it reasonable to assume that the directors had inside director knowledge for which they could be held liable.[24]

Similarly, in *Tischler v. Baltimore Bancorp*[25] a class action brought by purchasers of Baltimore Bancorp stock alleged, in relevant part, that the outside directors were liable under Section 10(b) of the Exchange Act and Rule 10b-5, for a purportedly false press release about the adequacy of an offer for the company. In evaluating the defendants' motion to dismiss, the Court dove into the different types of directors and their level of regular briefings. For this reason, audit committee members substantively briefed about the purchase offer had liability. The judge did not stop there, however. Where the outside directors had special knowledge of the company's field the judge concluded that they knew, or should have known, of the risks to the company.[26]

We would also add that certain specialised industries may have pitfalls that will increase the risk of director liability. A good example is the franchise industry. Specifically, if franchisors prescribe the technology that franchisees must use (including for payment card processing), they must ensure that the technology they prescribe is sufficiently secure and kept up to date. This lesson was learned by Sonic Drive-In. After its 2017 data breach, in which hackers stole customer payment card information from more than 700 Sonic franchised Drive-Ins, consumers brought a class action in the Northern District of Ohio. Sonic then moved for summary judgment on the negligence claim. The Court found that under Oklahoma law, parties generally do not have a duty to "anticipate and prevent the intentional or criminal acts of a third party" but can be held responsible for a data breach if their "own affirmative act has created or exposed [plaintiffs] to a recognizable high degree of risk of harm through such misconduct, which a reasonable [person] would have taken into account".[27] The court found four possible "affirmative acts" there that warranted a trial because of the manner in which the technology was imposed upon franchisees by the franchisor.[28]

Second-guessing board decision-making

As mentioned above, some of these risks flow directly from the content of public disclosures but others come from evaluating the objective quality – in light of the attendant circumstances – of officer and director decisions. Officers and directors have a duty of care to the corporation. "Duty of care" refers to a fiduciary responsibility held by company directors to live up to a certain baseline standard of care. This ethical and legal duty requires officers and directors to render their decisions in good faith and in a reasonably prudent manner. That second clause, "reasonably prudent manner", provides the legal ammunition to second-guess failed decisions. Shareholders can probe the reasonableness of officer-and-director decision-making by bringing shareholder derivative actions. These derivative actions argue that officers and directors violated their duty of care when it comes to one or more decisions and therefore injured the company itself. The areas of decision-making failures have run the gamut from poor business decisions, to accounting fraud, to bribery, to rampant officer looting, and – increasingly – failures to provide adequate cybersecurity safeguards.

The Delaware Chancery Court held in *In re Caremark International Inc. Derivative Litigation*[29] (*Caremark*), that the board has an obligation to at least attempt in good faith to invest in or implement a monitoring system that is sufficient to identify legal breaches by the corporation. In *Caremark*, shareholders brought derivative suits against the company, alleging that Caremark's directors breached their duty of care by failing to adequately oversee the conduct of Caremark's employees regarding kickback payments to doctors for Medicare or Medicaid referrals – which is a crime – thereby exposing the company to significant civil and criminal penalties. *Caremark*'s holding outlined director liability for a breach of the duty to exercise appropriate care in two distinct contexts: (1) "from a board decision that results in a loss because that decision was ill advised or 'negligent'"; or (2) "from an unconsidered failure of the board to act in circumstances in which due attention would, arguably, have prevented the loss".[30] The *Caremark* court further held that: "it is important that the board exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility." While all of these individual parts of the *Caremark* decision are important, the board must have failed to provide reasonable oversight in a "sustained and systematic fashion", or the information reporting system must be an "utter failure".

Cybersecurity crises of all stripes, including (but not limited to) ransomware response, have now become a staple of derivative lawsuits. Indeed, these claims have become so prevalent that we now have formal court opinions holding that derivative actions against boards for ransomware failures constitute the types of central case that must be covered by directors and officers (D&O) liability insurance.

This does not mean that the cases are always successful. For example, in *Corporate Risk Holdings LLC, v. Rowlands*,[31] the court concluded that case solely "amounts to an allegation that the Board knew about the risk posed by a cyberattack, but did not adequately monitor [the company]'s cybersecurity efforts".[32] Where plaintiffs "focus on a specific, industry-wide risk [the allegations are]… not sufficient to support a *Caremark* claim".[33] For example, directors of banks who failed to recognise the risks associated with the subprime lending market could not be found, merely by ignoring the publicised risks, to have acted in bad faith.[34]

Still, there must be a reporting system so that the board can exercise oversight, and companies often have weak reporting systems. Recently, the Delaware Chancery Court in *In re the Boeing Company Derivative Litigation*, suggests important steps organisations and their boards should take to help protect themselves from shareholder litigation-based security or compliance incidents.[35] This particular litigation arises from two crashes of 737 MAX airplanes manufactured by Boeing in October 2018 and March 2019. Investigations revealed that: (a) the 737 MAX tended to pitch up due to its engine placement; (b) a new software program designed to adjust the plane downward depended on a single faulty sensor and therefore activated too readily; and (c) the software program was insufficiently explained to pilots and regulators. In both crashes, the software directed the plane down. Because this was a derivative action alleging that the board was at fault, the question before the Court was whether "the Company's directors face a substantial likelihood of liability for Boeing's losses" based either on "the directors' complete failure to establish a reporting system for airplane safety", or based on "turning a blind eye to a red flag representing airplane safety problems". The Court concluded that the shareholders sufficiently pled both sources of liability.

One can easily translate plaintiffs' core allegations in Boeing into the arena of cybersecurity and data privacy: (1) "[t]he Board had no committee charged with direct responsibility to monitor airplane safety"; (2) "[t]he Board did not monitor, discuss, or address airplane safety on a regular basis"; (3) "[t]he Board had no regular process or protocols requiring management to apprise the Board of airplane safety; instead, the Board only received *ad hoc* management reports that conveyed only favorable or strategic information"; and (4) "[m]anagement saw red, or at least yellow, flags, but that information never reached the Board". These allegations alone suffice to raise the spectre of officer and director liability and many companies could be described in the same manner.

With these standards in mind, organisations should ensure that appropriate processes are in place to keep boards and management timely and adequately informed about cybersecurity risks that might impact the company. Organisations should also consider providing board members and management with an appropriate level of D&O insurance to help protect these leaders in the event of such litigation, and so that talented management is not deterred from taking such important oversight positions. Most importantly, companies and their management should embrace an agile approach to these issues. The goal of a company is not to hope that things stay the same. Rather, the dynamic, forward-thinking company tries to anticipate the next risk before their directors face personal liability.

However, for now, directors can and should allege that all such allegations of the breach of cyber duty of care constitute "a classic example of the difference between allegations of a breach of the duty of care (involving gross negligence) as opposed to the duty of loyalty (involving allegations of bad-faith conscious disregard of fiduciary duties)".[36] These standards are even more daunting for plaintiffs when "the claims involve a failure to monitor business risk, as opposed to legal risk".[37]

Special director knowledge, Delaware law, and the Section 141(e) "safe harbor"

Delaware case law paints a slightly different outlook as to whether independent directors will be held to a higher fiduciary duty standard because of their special expertise. The *In re Citigroup Inc. Shareholder Derivative Litigation*[38] showed that audit committee financial experts on the board violated their fiduciary duties by allowing the company to engage in subprime lending. The Delaware Chancery Court stated that "[d]irectors with special expertise are not held to a higher standard of care in the oversight context simply because of their status as an expert".[39] Rather than a failure of management oversight, the court viewed the operative issue as a failure to recognise a business risk, emphasising that "[e]ven directors who are experts are shielded from judicial second guessing of their business decisions".[40]

A similar "business decision" deference did not apply to the court's decision regarding *In re Emerging Communications, Inc. Shareholders Litigation*,[41] wherein a director with financial expertise was held to have a duty to voice concerns about the fairness of a proposed transaction's price. The meaning of this case has been widely debated. One interpretation is that, although directors possessing special expertise might not be held to a higher standard under Delaware fiduciary duty law, they may lose the safe harbour protection afforded by Section 141(e) of the Delaware General Corporation Law.

Section 141(e) provides that a director's good faith reliance upon "such information, opinions, reports or statements presented to the corporation...as to matters the member reasonably believes are within such other person's professional or expert competence and who has been selected with reasonable care..." will be afforded legal and factual deference. However, if a director has a particular expertise, then he or she may be unable to rely in good faith on an expert's report (or omission). As companies' SEC proxy disclosures expand upon directors' particular qualifications and expertise, they also effectively limit the scope of Section 141(e) deference. Where a director's cyber *bona fides* are trumpeted, even under Delaware law, they will enjoy less "business decision" deference in matters involving cybersecurity.

There is currently tension developing between these director disclosures, which grow ever more elaborate and more prominent, and the protections of the "business decision" deference. If nothing else, civil plaintiffs may endeavour to weaponise a director's publicly touted expertise to argue that the same director either violated the federal securities laws or his or her fiduciary duties. While all such claims require proof (in this specific context) of the director's knowledge about specific cybersecurity risks, a company's own admissions about a director's cybersecurity knowledge and expertise make the cases easier to allege and prove. Drafting these director cybersecurity disclosures has therefore become a high-stakes balancing act: companies must provide truthful and informative disclosures while also taking care to keep those disclosures lean enough to not create greater litigation risks.

The changes in legal risks appear to *In National Ink and Stitch, LLC v. State Auto Property and Casualty Insurance Company*,[42] a federal court held that a ransomware attack was covered by standard business loss language in a contract. In other words, the risks of a cyber event are so commonplace that any mention of business risk should contemplate these types of losses.

California liability

The California Consumer Privacy Act (CCPA) came into effect on January 1, 2020. The CCPA gives California residents expansive rights[43] over businesses' collection, use and sharing of their personal information. The CCPA: (1) vests general enforcement

authority with the California Attorney General (AG);[44] and (2) creates a private right of action that can only be brought against certain data breach incidents "and shall not be based on violations of any other section of" the CCPA.[45] *More than 50 lawsuits were filed in the first six months after the CCPA came into effect.* Roughly half of these lawsuits related to data breaches. The CCPA created no other types of civil or regulatory liability. However, the CCPA has been used to augment certain existing civil liability theories.

Plaintiffs in the other cases premise claims on alleged violations of consumer rights, often asserting that non-compliance with the CCPA, by extension, constitutes a violation of California's Unfair Competition Law (UCL), Consumer Legal Remedies Act (CLRA) or other causes of action. Many of the suits, whether for data breach or hybridised with another theory, were filed as class action lawsuits.

CCPA enforcement against directors

As mentioned above, the AG has broad authority to enforce all violations of the CCPA. Businesses that violate the CCPA will be subject to civil enforcement actions by the AG. Violating businesses will be given a notice of non-compliance and a 30-day opportunity to cure the non-compliance. Businesses who fail to comply within the 30 days will be subject to an injunction and a civil penalty: $2,500 for each unintentional violation; and $7,500 for each intentional violation. Because of the nature of privacy and cybersecurity events, these violations, and the related penalties, can compound quickly.

The AG has exercised broad authority to enforce California laws against directors in the past.[46] However, enforcement of the CCPA only began on July 1, 2020. The regulations issued after enforcement began.[47] These regulations provide no insight as to whether the AG will seek to hold officers and directors personally liable for a company's violations. Furthermore, active enforcement is still so new that we have few cases to examine that would suggest such authority will be exercised in the future. In general, officers and directors should be aware of the risk that the AG will seek to utilise the CCPA against them if there are systemic failures under that statute.

CCPA civil suits filed in connection with data security incidents

Most CCPA civil cases allege a data breach and then generally contend that the breach was a violation of the CCPA without offering additional details.[48] The CCPA claims usually join negligence, breach of contract, unjust enrichment and violation of the UCL claims.[49] Other cases include greater factual and procedural specificity.[50] However, thus far, none of these cases have sought to hold the officers or directors personally liable.

A number of cases also assert a violation of California's UCL *based upon* a data breach violating the CCPA.[51] The UCL defines "unfair competition" broadly to "mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by [California's false advertising law]". While these cases may seek injunctive relief and restitution, they, like the pure CCPA cases, have not yet articulated any claims against the officers and directors.

These class action cases are not the only types of civil liability that may draw upon the CCPA. One recently filed case is between competing businesses engaged in market research that involves the collection and sale of personal information.[52] The plaintiff alleges that the defendant (the plaintiff's former business partner and now competitor) violated the CCPA by failing to provide sufficient notice of its privacy practices to consumers, and as a result, has gained an unfair and unlawful advantage in violation of the UCL. It is not hard to see insider directors wrapped up in similar theories.

Alleging compliance with the CCPA could even form the basis of some of the derivative actions based upon fiduciary duties discussed earlier. Basically, such cases would allege that violating the CCPA constitutes a gross dereliction of oversight that amounts to a breach of fiduciary duties. Cases utilising these cases are coming but, as we shall see below, the cases filed thus far have not reached a high level of sophistication.

Privacy litigation under the CCPA

In 2021, CCPA liability appears to have been firmed and broadened. For example, it may be safe for an organisation to state on its website and public disclosures that it "take[s] privacy and security seriously" and it is "[d]edicated to maintaining the highest security standards" because this is mere "puffery". However, things become actionable quickly. A claim that the organisation uses "security measures that comply with federal law", however, can be actionable because "a reasonable consumer could rely on this statement as representing that [the organization's] safeguards, which were represented to comply with federal law, were sufficient to protect users' information from ordinary data security threats".[53] In this case, plaintiffs alleged that "[c]ontrary to its representations, [the organization did] not keep its promise to use security measures that comply with federal laws", because the organisation's systems: (a) "lack[ed] simple and almost universal security measures used by other broker-dealer online systems"; (b) "fail[ed] to verify changes in bank account links"; and (c) "failed to store user credentials in an encrypted format". The court found that these allegations were sufficient to withstand a (second) motion to dismiss.

In March 2020, plaintiffs filed *Cullen v. Zoom Video Comm., Inc.*[54] Since filing, the judge in this Northern District of California federal civil action related and consolidated separate actions. This recaptioned Frankenstein monster of a class action lawsuit claims that Zoom illegally shared millions of users' personal information with Facebook and failed to protect their personal information, thus violating the CCPA. Plaintiffs also allege that Zoom's privacy policy contained misrepresentations, that Zoom made inadequate privacy notices about its data collection and use, and that Zoom failed to implement and maintain reasonable security procedures and thus committed fraud in violation of the UCL. The lawsuit also alleges violations of California's CLRA and of California consumers' constitutional privacy rights. The viability of these claims will not be tested soon: a hearing on class certification is scheduled for May 27, 2021.

The *Consolidated Ambry Genetics Cases*[55] are the collective name for the consumer class action cases filed against genetic testing company Ambry Genetics for a January 2020 data breach. Plaintiffs allege that the breach resulted in unauthorised access to customers' personally identifiable information and protected health information, and that Ambry failed to timely report the breach to the government or to customers. These cases were consolidated in June 2020. Despite the wide variety of legal theories on display here, none of the *Consolidated Ambry Genetics Cases* articulate personal liability claims against the officers or directors. The same is true for *Gupta v. Aeries Software, Inc.*,[56] wherein plaintiffs allege that Aeries did not adequately safeguard the personally identifiable information of thousands of vulnerable students, resulting in unauthorised third parties accessing that data. *G.R. v. TikTok*[57] provides yet another CCPA lawsuit that fails to bring claims against the officers and directors. While this case does not directly impact them, officers and directors should take note of the data security and privacy issues that are explored in this case, which alleges unlawful harvesting of biometric identifiers from minor and adult users. These types of issues do not seem to involve data security or privacy, but the

laws and regulations – including the CCPA – increasingly cover both biometrics and the protection of minors. The lawsuits will follow the same path as these laws and regulations.

Other state liability

New York State

The NYDFS, which is responsible for the regulation of banks, insurers and other financial institutions that do business in New York, has a growing role in pushing cybersecurity standards. The NYDFS also possesses an expansive view of its own jurisdictional limits, the entities that it regulates, and their respective officers and directors.

New rules developed by the NYDFS under 23 NYCRR Part 500 (the Regulation), which came into effect on March 1, 2017, require entities that NYDFS regulates to implement specific cybersecurity standards. These standards include establishing a comprehensive cybersecurity policy, completing a written incident response plan (focusing upon reporting breaches within 72 hours to the NYDFS), and promulgating security policies for third-party vendors. The rules require officers and directors to not only designate a chief information security officer (CISO), but also to certify to the NYDFS that the company is in compliance with the regulations.

The CISO must prepare an annual report to the board of directors of the regulated entity regarding its cybersecurity program. The report must: (1) specifically address the identification of material cyber risks to the regulated entity, including any past material cybersecurity event; and (2) report on penetration testing and vulnerability assessments. The CISO must also report to the board of directors about, *inter alia*, multifactor authentication and cyber awareness training for all personnel. In short, the boards of covered companies likely received far more cyber information than they ever received prior to the NYDFS rules. With this deep cyber information in hand, officers and directors were required to submit the first cybersecurity compliance certification to the NYDFS by February 15, 2018. This is a yearly requirement[58] that will annually put directors into the cybersecurity weeds. Moreover, by certifying compliance with these detailed cybersecurity requirements, directors become primary targets of these regulators if a breach occurs.

Other states

A number of other states are considering enhanced cybersecurity and privacy regulations. In the privacy sphere, many states are considering adopting aspects of California's sweeping CCPA. Other states, like Washington, are likely to adopt a framework similar to that utilised by the EU,[59] discussed in further detail below. In any case, the two main risks to directors are the same as they are in California: (1) enforcement actions against officers and directors brought by individual state attorneys general; and (2) private actions alleging either substantive violations of the statute or qualitative violations of the duty of care premised upon a failure to comply with the statute.

Global Personal Cyber Risks for Officers and Directors

New legislation in a range of jurisdictions, most notably in the EU under the new General Data Protection Regulation (GDPR),[60] will hold organisations to higher cybersecurity and cyber standards than ever. With those growing risks in mind, it is useful to consider the potential liability landscape in all jurisdictions in which they are active.

The UK

In the UK, directors' fiduciary duties to the company are largely codified under the Companies Act 2006 (the 2006 Act).[61] Among other things, directors of UK companies possess a duty to promote the success of the company and to exercise reasonable care, skill and diligence in the conduct of their role.[62] Similar to United States civil liability theories, the board's failure to understand and mitigate cyber risks could constitute a breach of these duties. In evaluating these types of claims, UK law requires that we consider the standard of a reasonably diligent person with the knowledge and skill of the director in question. These standards will be tested, as in the United States, via derivative actions.

Recent UK case law has established that civil lawsuits may be brought against violations of the UK Data Protection Act 1998.[63] Perhaps most concerning to companies assessing their civil cyber risks in the UK, is that these Data Protection Act cases can proceed even when the plaintiff has not suffered pecuniary loss. Stated differently, companies face civil losses even where they did not cause anyone to actually lose money. These UK cybersecurity and privacy lawsuits may be brought against the company or the individual directors.

Doing business in the UK will also expose companies to the GDPR. The UK's "Brexit" from the EU will not alter the applicability of the GDPR. The GDPR imposes broad regulations upon companies that control or process personal data. Penalties for GDPR violations can be staggering: non-compliance penalties extend up to the higher of €20 million or 4% of the organisation's worldwide revenue. Moreover, directors of public companies bear the responsibility for compliance with the GDPR and personal liability for any fines and penalties.[64] In addition, the Information Commissioner's Office, the UK's data privacy regulator, can compel future conduct from senior board members to ensure that the company complies with its ongoing data protection obligations.

Directors of regulated entities also need to be aware of their UK personal regulatory obligations. In the financial services sector, the Financial Conduct Authority closely scrutinises directors, and will take action if a director fails to discharge his or her regulatory duties as a result of not properly managing the organisational cyber risks. Similarly, directors of publicly traded companies must appropriate disclosures under the UK Listing Rules. These disclosures may include a wide range of adverse cyber events. Directors face personal liability for any failure to disclose such events.

The EU

In addition to the GDPR, which we discussed with regard to the UK, the EU is developing a number of new laws and regulations regarding cybersecurity and privacy. For example, the EU Network and Information Security Directive (NIS Directive)[65] will require companies in certain industries (including such far-flung industries as financial services and "water transport")[66] to implement certain minimum cybersecurity standards. While enforcement of the NIS Directive is still unclear, and its effectiveness is under review as of October 2020, the mere fact that the NIS Directive will be implemented in the EU should alter the way that directors think about cybersecurity implementation.

Ireland's Data Protection Commission recently announced a whopping €225 million fine against WhatsApp for allegedly failing to comply with GDPR transparency requirements.[67] The fine follows a lengthy July 28, 2021 decision issued by the European Data Protection Board. The decision was largely driven by the extent to which "hashed" consumer data constitutes "personal

data" for the purposes of the GDPR. Among other things, the answer seems to depend upon "when" the data is hashed and whether or not the hashing "guarantee[s] the anonymisation of data". These fine distinctions further raise the heat on companies.

Amazon announced in August 2021 that it had been hit with a record $888 million fine for purportedly violating the GDPR. In its July 30 SEC 10-Q filing, Amazon stated that "On July 16, 2021, the Luxembourg National Commission for Data Protection [the "CNPD"] issued a decision against Amazon Europe Core S.à r.l. claiming that Amazon's processing of personal data did not comply with the EU General Data Protection Regulation. The decision imposes a fine of €746 million and corresponding practice revisions. We believe the CNPD's decision to be without merit and intend to defend ourselves vigorously in this matter." 10-Q at 13. The CNPD Complaint apparently alleges that Amazon analyses users' behaviour to build profiles for targeted advertising without user consent and in violation of the GDPR.

Germany

German law provides similar personal liability pitfalls for directors. Under German law, directors can be held liable for breach of their duties. These cybersecurity duties include, *inter alia*, a duty to ensure that there is adequate IT infrastructure to protect data security and to avoid cyber risks. Directors must therefore ensure that certain technical standards are met, which are actually spelled out in the German Data Protection Act (*Bundesdatenschutzgesetz*) and the German IT Safety Act (*Bundessicherheits- und Informationstechnikgesetz*). The German laws also require a high level of ongoing systems monitoring. This can mean that the failure to note intrusions, which can sometimes last months, can itself constitute an organisational failure. While all of these regulatory responsibilities should concern directors, it bears noting that German law generally only permits director liability to the company not to third parties, although the risk exists.

United Arab Emirates

Under United Arab Emirates (UAE) law, officers and directors of a company can face personal liability for matters relating to cyber risk. The board of directors of a public joint stock company is liable to the company, its shareholders and third parties for certain acts, including fraud, misuse of power, breach of the UAE Commercial Companies Law or the company's articles of association, or an error in management.[68] While little case law exists on how these provisions may be applied, there is a possibility that cybersecurity and privacy failures may fall under the law.

Of more concern should be potential criminal liability under UAE law. Officers and directors should be mindful that potential criminal liability exists for the unauthorised disclosure of personal information. Reportedly, in March 2015, three executives in the UAE were all temporarily imprisoned on the grounds of a breach of privacy in connection with the installation of CCTV. Jail time is therefore a real possibility in the UAE.

Canada

Canadian law can impose personal liabilities upon officers and directors of a company for matters relating to cybersecurity and privacy risk under Canadian law. The Canada Business Corporation Act RSC 1985 (CBCA) requires every director to exercise their powers and duties honestly and in good faith, with a view to the best interests of the corporation; and exercise the care, diligence and skill that a reasonably prudent person would exercise in comparable circumstances.[69] The CBCA provides for shareholder derivative actions for breaches of duties owed by directors to the company and the recovery of monetary damages on behalf of the company.[70] Thus, in theory, companies operating in Canada bear many of the same litigation risks for their cybersecurity and privacy failures.

As in the United States, Canada imposes liability upon directors for omissions or misrepresentations in public disclosures. Moreover, since September 2013, the Canadian Securities Administrators have instructed that issuers should expressly disclose their cyber-crime risks, any cyber-crime incidents, and characterise their cybersecurity controls in a prospectus or a continuous disclosure filing.[71]

Officers and directors also face statutory liabilities for under privacy statutes in Canada. These statutes only exist in certain discrete Canadian jurisdictions, however. Breaching Quebec's privacy statute can lead to monetary fines against directors who ordered or authorised the breaches.[72] Likewise, Ontario's Personal Health Information Protection Act 2004 contains penalties to officers and directors for the wilful collection of health information without reasonable protections.[73]

South Africa

South African law also creates personal liabilities for officers and directors in connection with cybersecurity and privacy risks under South African law. As in other countries utilising a derivation of the English legal system, the failure to implement reasonable cybersecurity measures could constitute a breach of directors' fiduciary duties. As in countries like the United States and England, these fiduciary duties were established by way of the common law and have later been codified. Just as in these other countries, officers and directors have a duty to maintain certain minimal cybersecurity and privacy procedures and oversight. Officers and directors could theoretically face personal liability to the company and to third parties for a breach of these duties. A breach of directors' fiduciary duties could lead to claims being brought against officers and directors. Similarly, just as in the UK and the United States, directors may face personal liability in contract or tort. This risk is even more acute in South Africa, where the governing laws permit great personal liability, even when working through the "legal fiction" of a corporation.

Moreover, a breach of fiduciary duty could lead to South African regulators taking action against officers and directors. For example, the Companies and Intellectual Property Commission (CIPC). The CIPC can investigate these complaints and various mechanisms allow action to be taken against a company or its directors.

Common law, rather than a statute, primarily protects the South African right to privacy However, South Africa has also passed the Protection of Personal Information Act, of 2013 (POPI).[74] Under the POPI, regulatory action may be taken against an organisation or person for any violation. Therefore, depending on the nature of each violation, a director may face civil fines, administrative fines, penalties and even a period of imprisonment. The POPI does not fully become effective until July 2021, which is when the "grace period" ends.

Australia

As in the UK, United States, and South Africa, officers and directors face certain familiar personal liability risks for a company's cybersecurity and privacy failures. All officers and directors have

a key responsibility to ensure that companies adopt appropriate risk management strategies to protect the company and its shareholders via their duty of care and due diligence, under both Section 180 of the Corporations Act 2001[75] and the common law. The Australian corporate regulator, the Australian Securities and Investments Commission (ASIC), has the power to bring an action against officers and directors for a breach of their duties. The consequences are potentially serious, and include a declaration of contravention, pecuniary penalties, compensation orders and disqualification of the director or officer from managing a corporation. ASIC Report 429[76] states that: it considers board participation important to promoting a strong culture of cyber resilience; and a failure to meet obligations to identify and manage cyber risks may result in stiff penalties. Finally, a failure by officers and directors to take reasonable steps to prevent, or respond appropriately to, a cyber or privacy incident may also give rise to Australian civil proceedings, either via derivative action brought by the shareholders or by affected individuals.

Emergent Areas of Special Cybersecurity and Privacy Concern to Officers and Directors

Data and privacy security is not just the target of criminals. Foreign governments utilise their military and intelligence resources to actively attack the privacy and data assets of private companies. These state actors carry special risks that officers and directors must acknowledge. For example, Chinese military hackers stole U.S. Steel's trade secrets and gave them to Chinese steel companies so that they could better compete in western markets.[77] U.S. Steel attempted to meet this threat by filing an action in the International Trade Court.[78] After a long and costly fight, U.S. Steel withdrew its cybertheft action, but the legal fight is far from over.[79] Whenever nations endeavour to interfere with businesses, the officers and directors should take note.

State actor privacy and data security concerns can even lead to the forced liquidation of assets. The saga of TikTok is well known at this point. However, it bears repeating that the United States' insecurity about the state of TikTok's privacy and data security procedures and controls has led directly to a likely "forced" liquidation of United States assets. Russia's potential control over private data led to similar insecurity over the viral FaceApp.[80] In other words, state actors are now colliding with data security and privacy in a manner that provides an existential threat to many companies. Where the risks to companies are great, the personal liability risks to officers and directors can be correspondingly large.

Certain business sectors can also face outsized risks of which officers and directors must be aware. If a company services sensitive or classified governmental contracts, they will be both a target of bad actors and also subject to increased regulatory oversight. The dimensions of those standards, whether under the Defense Federal Acquisition Regulation Supplement (DFARS) cybersecurity requirement or under government contracting requirements that the National Institute of Standards and Technology (NIST) guidelines be met, should be the subject of a different article. However, for our purposes, we should acknowledge that officers and directors must be aware that these standards exist – and work to satisfy them – or else they face the loss of extremely valuable contracts.

Not only traditional defence or governmental industries face these threats. State-sponsored hackers hacked Yahoo![81] and the World Anti-Doping Agency.[82] Zappos was hacked by a hacker who works for the successor to the KGB.[83] While Zappos is a very successful online commerce company, one would not usually think of them as a geopolitical target – that is all changing. Similarly, as discussed above, one response to the ransomware threat has been to sanction certain ransomware payments, which means the expedient act of paying ransomware may now place officers and directors at odds with the OFAC. This is a significant wrinkle that further complicates companies' decisional calculus. Officers and directors must address these risks now or they face the prospect of personal liability for their failures later.

Endnotes

1. https://www.sec.gov/news/press-release/2018-22.
2. https://www.sec.gov/news/press-release/2018-71.
3. https://www.sec.gov/rules/interp/2018/33-10459.pdf; see also 17 CFR 243.100. Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (August 15, 2000) [65 FR 51716 (August 24, 2000)].
4. Proxy Disclosure Enhancements, SEC Release Nos 33-9089, 34-61175, IC-29092; 74 FR 68334 (December 23, 2009).
5. Disclosure Required by Sections 406 and 407 of the Sarbanes-Oxley Act of 2002, SEC Release Nos 33-8177, 34-47235; 68 FR. 5110 (January 31, 2003).
6. Director liability under the operative sections of the federal securities laws turns on the director's knowledge or the reasonableness of his or her beliefs in a specific situation and can presumably be impacted by his or her particular qualifications, background or expertise. A director has a "due diligence" defence to liability under Section 11 if he or she sustains the burden of proof that, with regard to any part of the registration statement not made under the authority of an expert, the director "had, after reasonable investigation, reasonable ground to believe and did believe, at the time such part of the registration statement became effective, that the statements therein were true and that there was no omission to state a material fact". Federal courts have generally taken the view expressed in *Feit v. Leasco Data Processing Equipment Corp.*, 332 F. Supp. 544, 577 (E.D.N.Y. 1971) that "[w]hat constitutes 'reasonable investigation' and a 'reasonable ground to believe' will vary with the degree of involvement of the individual, h[er] expertise and h[er] access to the pertinent information and data". Thus, directors who are insiders, or directors who are attorneys involved in preparation of the registration statement, generally are expected to make a more complete investigation and have more extensive knowledge of the facts at issue.
7. https://www.sec.gov/news/press-release/2021-154.
8. 17 CFR 229.407(h); 17 CFR 240.14a-101 – Schedule 14A.
9. Final Rule: Proxy Disclosure Enhancements, Release No. 33-9089 (December 16, 2009) [74 FR 68334 (December 23, 2009)], available at http://www.sec.gov/rules/final/2009/33-9089.pdf.
10. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos 33-10459; 34-82746, (February 26, 2018), available at https://www.sec.gov/rules/interp/2018/33-10459.pdf.
11. https://www.sec.gov/news/press-release/2021-176.
12. https://www.sec.gov/news/press-release/2021-169.
13. https://www.sec.gov/litigation/complaints/2018/comp-pr2018-40.pdf, https://www.sec.gov/litigation/complaints/2018/comp-pr2018-115.pdf.
14. https://www.sec.gov/news/testimony/testimony-oversight-us-securities-and-exchange-commission.
15. *Id.* at 3-4.
16. https://www.finra.org/rules-guidance/notices/21-29.
17. https://www.federalreserve.gov/newsevents/pressreleases/bcreg20210713a.htm.
18. Section 141(a), Delaware General Corporation Law.

19. *Graham v. Allis-Chalmers Mfg Co.*, 188 A 2d 125, 130 (Del 1963).
20. *Smith v. Van Gorkom*, 488 A 2d 858, 872 (Del 1985).
21. *Stone v. Ritter*, 911 A 2d 362, 370 (Del 2006).
22. 806 F. Supp. 1197 (E.D. Pa. 1992).
23. *Id.* at 1203.
24. *Id.* at 1204.
25. 801 F. Supp. 1493 (D. Md. 1992).
26. *Id.* at 1501.
27. https://media-exp1.licdn.com/dms/document/C4D1FAQEv_akeXkjhTQ/feedshare-document-pdf-analyzed/0/1631188958350?e=1632236400&v=beta&t=S4tMjTX3B4d-KhDSWkcNMsdOGgdy85TV7V7ZkQGtCSMI.
28. First, "Sonic created a permanently-enabled VPN tunnel that did not block foreign IP addresses that gave [its required POS vendor] and anyone with [its] credentials—access to each [POS]-served franchise point-of-sale systems". Second, "Sonic created, [a] remote user credential [for its POS vendor]...without multi-factor authentication enabled". Third, Sonic "required franchisees to use middleware that did not support point-to-point encryption". Finally, Sonic "controlled middleware upgrades, and caused delays that left franchisees operating vulnerable systems".
29. 698 A.2d 959 (Del. Ch. 1996).
30. *Id.*
31. No. 17-cv-5225(RJS), 2018 WL 9517195 (September 29, 2018).
32. *Id.* at *6.
33. *Id.* (citing *In re Citigroup Inc. S'holder Derivative Litig.*, 964 A.2d 106, 128 (Del. Ch. 2009)) ("[A] showing of bad faith is a necessary condition to director oversight liability".)
34. *In re Citigroup Inc. S'holder Derivative Litig.*, 964 A.2d at 112 ("[A] showing of bad faith is a necessary condition to director oversight liability".)
35. https://casetext.com/case/in-re-the-boeing-co-derivative-litig.
36. *In re Gen. Motors Co. Derivative Litig.*, C.A. No. 9627-VCG, 2015 WL 3958724, at *17 (Del. Ch. June 26, 2015).
37. *Wayne Cty. Emp.'s Ret. Sys. v. Dimon*, 629 F. App'x 14, 15 (2d Cir. 2015).
38. 964 A.2d 106 (Del. Ch. 2009).
39. *Id.* at 128 n.63.
40. *Id.*
41. C.A. No. 16415, 2004 BL 1814 (Del. Ch. May 3, 2004).
42. 435 F.Supp.3d 679 (D. Md. 2020).
43. The Act provides California residents with the right to seek access to, or deletion of, their personal information, as well as the right to object to the sale or sharing of such information with third parties.
44. See Cal. Civ. Code § 1798.155(b).
45. See Cal. Civ. Code § 1798.150(c) ("The cause of action established by this section shall apply only to violations as defined in subdivision (a) [regarding data breaches] and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.")
46. https://oag.ca.gov/news/press-releases/attorney-general-sues-remove-stakeholder-members-iso-board.
47. https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf.
48. See, e.g., Complaint, *Albert Almeida, Mark Munoz, and Angelo Victoriano v. Slickwraps Inc.*, No. 2:20-at-00256, at 28, 48 (E.D. Cal. March 12, 2020); Complaint, *Daniela Hernandez v. PIH Health*, No. 2:20-cv-01662, at 6, 19, 38 (C.D. Cal. February 20, 2020); Complaint, *Bernadette Barnes v. Hanna Andersson, LLC, and Salesforce.Com, Inc.*, No. 4:20-cv-00812-DMR, at 3, 15 (N.D. Cal. February 3, 2020); Complaint, *Juan Maldonado v. Solara Medical Supplies, LLC*, No. 3:19-cv-02284-H-KSC, at 3, 21 (S.D. Cal. November 29, 2019).
49. See, e.g., Complaint, *Slickwraps* at 39, 44, 46 and 48; Complaint, *Hernandez* at 22, 27, 30 and 37; Complaint, *Barnes* at 16 and 22; Complaint, Maldonado at 23, 30, 33 and 34; see also *Rahman v. Marriott International, Inc.*, Case No. 8:20-cv-00654 (C.D. Cal. April 3, 2020) (This putative class action on behalf of California residents against Marriott for a data breach that was announced on March 31, 2020 alleges violation of the CCPA and UCL, as well as breach of contract and implied contract, negligence, and unjust enrichment.)
50. See, e.g., Complaint, *Michele Pascoe v. Ambry Genetics*, No. 8:20-cv-00838, at 50 (C.D. Cal. May 1, 2020) at 50; Complaint, *Lopez* at 44.
51. See, e.g., Complaint, *Slickwraps* at 48; Complaint, *Hernandez* at 37–38.
52. See Complaint, *Bombora v. ZoomInfo*, No. 20-cv-365858 (Cal. Super. Ct. June 10, 2020).
53. https://www.linkedin.com/posts/brian-levine-49579348_mehta-v-robinhood-nd-cal-sept-8-2021-activity-68420814-64369061889-jyRm.
54. Case No. 20-cv-02155 (N.D. Cal. March 30, 2020).
55. Case No. 8:20-cv-00791 (C.D. Cal.).
56. Case No. 8:20-cv-00995-FMO-ADS (C.D. Cal. May 28, 2020).
57. Case No. 2:20-cv-04537 (C.D. Cal.).
58. https://www.dfs.ny.gov/industry_guidance/cyber_filings/requirements.
59. https://fpf.org/2020/01/13/its-raining-privacy-bills-an-overview-of-the-washington-state-privacy-act-and-other-introduced-bills/#:~:text=The%20Act%20would%20be%20a,creates%20a%20nuanced%20approach%20to.
60. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
61. https://www.legislation.gov.uk/ukpga/2006/46/contents.
62. *Id.* (sections 172 and 174, 2006 Act).
63. *Google Inc v. Vidal-Hall and other* [2015] EWCA Civ 311 **.
64. Per the first and second paragraphs of Article 169, the members of the management board must act as thorough and diligent owners, and they are jointly and severally liable for the damage inflicted on company by their actions.
65. 2016/1148/EU**.
66. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.
67. https://lnkd.in/dbEF98Gx.
68. Article 162, UAE Federal Law No 2 of 2015 on Commercial Companies.
69. https://laws-lois.justice.gc.ca/eng/acts/C-44/page-21.html?txthl=duties+duty#s-122.
70. https://laws-lois.justice.gc.ca/eng/acts/C-44/page-41.html?txthl=derivative#s-239.
71. https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20130926_11-326_cyber-security.htm#:~:text=To%20manage%20the%20risks%20of,and%20their%20clients%20or%20stakeholders.
72. http://legisquebec.gouv.qc.ca/en/showdoc/cs/P-39.1.
73. https://www.ontario.ca/laws/statute/04p03.
74. https://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf.

75. http://www5.austlii.edu.au/au/legis/cth/consol_act/ca2001172/s180.html#:~:text=Care%20and%20diligence%2D%2Dcivil%20obligation%20only,-Care%20and%20diligence&text=The%20director's%20or%20officer,in%20their%20position%20would%20hold.
76. https://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf.
77. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
78. https://www.wsj.com/articles/u-s-steel-accuses-china-of-hacking-1461859201.
79. https://www.wsj.com/articles/u-s-steel-withdraws-hacking-claim-against-chinese-rival-1487183293.
80. https://www.pbs.org/newshour/science/is-faceapp-a-security-risk-3-privacy-concerns-you-should-take-seriously.
81. https://www.nytimes.com/2017/03/15/technology/yahoo-hack-indictment.html.
82. https://www.nytimes.com/2019/10/28/sports/olympics/russia-doping-wada-hacked.html.
83. https://www.forbes.com/sites/thomasbrewster/2017/03/20/alexsey-belan-yahoo-fbi-hacker-allegations/#bc236cd76f24.

Christopher Ott, CIPP/US, leads data security, privacy, and white-collar litigation and investigations. Leveraging his experience from more than 13 years at the U.S. Department of Justice (DOJ), including successfully litigating complex data security matters, conducting hundreds of investigations, and winning dozens of appeals, Mr. Ott works with clients on disputes and strategy relating to data security, privacy, blockchain, and AI issues. Mr. Ott has handled hundreds of matters involving the intersection between white-collar matters (accounting, securities, money laundering) and cybercrimes (from international criminal gangs to state actors). For example, much of his current work involves business litigation and investigative matters involving stablecoin and PoS blockchain technologies. In his most recent governmental role, Mr. Ott acted as Supervisory Cyber Counsel to the National Security Division of the DOJ. Mr. Ott consulted extensively with the intelligence community and coordinated extensively with regulators such as the U.S. Treasury Department, the Federal Communication Commission (FCC), the Federal Trade Commission (FTC), and the SEC.

Rothwell Figg
607 14th Street NW, Suite 800
Washington, D.C. 20005
USA

Tel: +1 202 783 6040
Email: cott@rfem.com
URL: www.rothwellfigg.com

The Privacy, Data Protection & Cybersecurity team at Rothwell Figg helps clients understand and navigate these rapidly evolving areas of law. We work with our clients to prepare, integrate, and implement compliance strategies, frameworks for risk management, and best practices. We have experience working closely with our clients: to build data inventories and assess their legal obligations; to implement back-end and structural changes that are not only compliant, but also workable; to prepare written policies, assessments, forms, and notices to effectuate legal requirements and best practices; to negotiate, draft, and review agreements for compliance; and to help train staff. We can assist with the design and implementation of incident response plans and, if there ever is an incident, we can serve as trusted advisors, from the investigation stages through to litigation, helping you navigate disclosure requirements to public authorities. Most of the attorneys in the practice group are experienced litigators with deep technical backgrounds, and have represented clients in a wide variety of venues, including before numerous government agencies, and in state courts, federal district courts and courts of appeal, and the United States Supreme Court.

www.rothwellfigg.com

ROTHWELL FIGG
IP Professionals

Cyber Capability to Evade International Sanctions: Problems, Solutions and Innovations

Ince


Julian Clark


Reema Shour

Executive Summary

In this chapter, we will consider the increasing use of advanced cyber capability to evade international economic and trade sanctions. This is discussed in the context of the wider threat that cyberattacks pose to the global economy and society as a whole.

We explain the use of international sanctions programmes as a political and economic tool to promote democracy and human rights and guard against other undesirable activities, such as terrorism and the proliferation of nuclear weapons. We summarise briefly the key international sanctions currently in place and against whom. We then address some of the principal methods used to evade international sanctions, concentrating in particular on the increasing use of cyberattacks and other cyber capabilities to bypass the international sanctions regimes in place.

Given the international maritime industry's highly significant contribution to the global economy and its key role in facilitating international trade and the global supply chain, we focus on the way in which various entities are using their cyber capability against the shipping sector for illegitimate purposes, including to evade sanctions. We highlight some of the cyber incidents that have impacted the international maritime sector and consider the principal ways in which the industry is addressing these ongoing cyber threats both to minimise sanctions evasions, but also to protect the industry generally from financial, reputational and operational harm.

Specifically, we discuss: industry guidance on maritime cybersecurity; legal risks that may result from lack of cyber preparedness; international regulations designed to combat and punish cyberattacks; practical problems arising; and some solutions that the maritime industry is implementing to minimise its cyber vulnerability and to enhance cybersecurity. We conclude by highlighting some initiatives designed to assist maritime organisations in maximising their cybersecurity.

The Origins and Purpose of International Sanctions Regimes

The international community has traditionally used a variety of financial, economic and trade sanctions against what are deemed "rogue states" and/or against designated individuals as a means of deterring a wide range of activities, including terrorism, non-constitutional government actions, the abuse of human rights and the proliferation of nuclear weapons. Implemented measures can take a number of different forms and can range from comprehensive economic and trade sanctions to more targeted measures, such as travel bans, arms embargoes, asset freezes, import and export restrictions, as well as embargoes on sensitive goods, such as software and technology that may be used, for example, to develop missiles and atomic weapons.

Sanctions may be imposed by the UN Security Council, the European Union and by individual states. The UK is a member of the UN Security Council and so it automatically imposes all financial sanctions created by the UN. The UK Government has also independently created a number of financial sanctions. Other nations will have similar sanctions programmes. The US, for example, has different sanctions programmes administered by the Office of Foreign Assets Control of the Department of the Treasury.

Key sanctioned regimes currently include Belarus, Iran, Myanmar, North Korea, Syria, Venezuela and Yemen. There are also sanctions in place against non-governmental organisations and groups, such as Al-Qaeda, ISIL/Daesh, under counter-terrorism initiatives.

Sanctions Evasion: Established Methods

Unsurprisingly, the more effective international sanctions regimes have become in curbing what the international community deems unacceptable activity that has national and international ramifications, the greater the proliferation of sanctions evasion methods designed to bypass and undermine prohibitions and restrictions. Indeed, and particularly in the light of increasingly sophisticated technology, sanctions evasion has become a major international concern.

There are a number of well-recognised methods of evading sanctions, for example: elaborate ownership structures such as front and shell companies to launder money and funnel it to sanctioned entities and/or to trade in prohibited goods; and, additionally, using a trade finance vehicle to move money without detection. Documents may also be falsified or altered to disguise the shipping route, the vessel used and the vessel's registration, the type of goods shipped, the entities and jurisdictions involved, etc.

Money laundering is also a widespread method of disguising otherwise illicit transactions. While established international financial institutions are obliged to have comprehensive anti-money laundering systems in place, anti-money laundering procedures are not infallible. By way of example, in 2018, Danish bank, Danske Bank A/S, faced civil penalties and possible criminal charges after its Estonian branch allegedly laundered several million dollars on behalf of sanctioned Russians and billions of dollars generally. While the US Department of Treasury ultimately concluded that Danske had not breached US sanctions and closed its investigation, the bank remained under investigation by various other countries as well as the US Department of Justice. The resulting reputational damage was enormous.

Sanctions Evasion: Cyber Hacks

Increasingly, those with sophisticated and advanced technological capabilities are using cyber hacks to evade sanctions. There are

a number of recent incidents whereby sanctioned entities and their facilitators have used their impressive cyber capability to undermine efforts aimed at bringing them into line.

Indeed, cyber-enabled money laundering is a potentially new and significant threat for financial institutions. The hacker uses a bank's computer system to execute a prohibited financial transaction by altering critical information or disabling anti-money laundering controls. It is effective because all the hacker has to do is disguise the illicit purpose or sanctioned participant of an otherwise legitimate transaction. This just requires the hacker to subtly alter customer data to avoid sanctions-screening lists or exempt an account from the focused scrutiny that banks apply to clients from sanctioned countries. Bypassed controls at a bank's overseas branches represent a particular risk. See, for example, the Danske Bank scandal referred to above that involved its Estonian branch.

In 2019, a UN Security Council panel of experts reported on North Korea's use of its sophisticated cyber capability to hack into central banks, corporate banks and cryptocurrency exchanges, as well as into ATMs around the world. The report noted that this method of evading sanctions had grown in sophistication and scale since 2016. One individual referred to in the report was charged by the US with a host of high-profile cyberattacks and was accused of involvement in the North Korean government-sponsored hacking team known as "Lazarus Group" linked to the 2017 WannaCry 2.0 global ransomware attack and also to a 2016 Bangladesh Bank theft of US$ 81 million. That report also documented at least five successful attacks against cryptocurrency exchanges in Asia between January 2017 and September 2018, resulting in losses estimated at US$ 571 million. Detection of such activities is not straightforward as financial institutions are often reluctant to admit that they have been hacked. The same report also accused North Korea of laundering funds through multiple jurisdictions and recommended implementing and promoting cybersecurity best practices.

Sanctions Evasion: Shipping Industry Targeted

The maritime industry accounts for around 80% of global trade by volume and over 70% by value. Consequently, illegal cyber activity within the global shipping sector is critical not only for the maritime industry but also for the world economy generally. Indeed, cyber hackers have recognised in recent years that the shipping industry is both a profitable but also a potentially vulnerable target, resulting in a reported 400% increase in attempted cyberattacks on shipping companies over a period of just five months in 2020. In 2019, a report from a Singaporean cyber risk management company suggested that a ransomware attack on Asian ports could cost the global economy as much as US$ 110 billion.

The risks are real and they extend worldwide. Between 2017 and 2020, the world's four largest shipping owners and operators suffered cyberattacks. Danish shipping company, APM Maersk, was hit by the NotPetya ransomware in 2017. In 2018, Chinese shipping line COSCO suffered a ransomware attack whose effects were felt for weeks. In 2020, Italian/Swiss shipping line Mediterranean Shipping Company was hit by an unnamed malware strain that knocked out its data centre for several days. In September 2020, a ransomware attack hit the IT systems of French shipping company CMA CGM and disabled its e-commerce systems for two weeks.

Increasingly too, illicit cyber activity in shipping is aimed at sanctions evasion. Indeed, the UN report referred to above indicated that North Korea had been conducting illicit ship-to-ship (STS) transfers of energy resources in violation of UN sanctions. There are also reports that Iran has been avoiding prohibitions on the import and export of Iranian oil by storing oil in large tankers at sea while finding potential buyers, then changing vessel names and identification codes to mask the identify of its oil tankers, making its vessels go "invisible" by disengaging ships' Automatic Identification Systems (AIS) and secretly moving oil through STS transfers to other, legitimate vessels.

How is the global maritime sector addressing these concerns? Through industry guidelines to ensure effective cyber risk management, through international and industry regulation and by implementing practical technological and other solutions. We consider each of these below.

Industry Guidance and Initiatives

In December 2020, the UK Treasury Office of Financial Sanctions Implementation (OFSI), published a maritime sanctions guidance that highlighted a number of suspicious and illicit shipping practices. These included a vessel's AIS being intentionally disabled in order to conceal the vessel's whereabouts, particularly in the case of STS transfers where the trade being conducted was illicit. Cyberattacks were also cited as a means of forcing the illegal transfer of funds from financial institutions and cryptocurrency exchanges to circumvent sanctions. Among other things, the OFSI recommended AIS screening and the incorporation of AIS switch-off clauses in contracts.

The US maritime industry has also recognised the adverse impact of cyberattacks and has sought to provide its recommendations on how to counter the threat. Indeed, the US Coast Guard (USCG) was hit with a Ryuk ransomware attack in December 2019 that shut down a maritime transport facility for 30 hours. The USCG has also made public its concern regarding leaked Iranian documents that allegedly detail research into how a cyberattack could be used to target critical infrastructure, including marine transportation entities.

In May 2020, the US Department of Treasury Office of Foreign Assets Control (OFAC) and the USCG issued an Advisory for the shipping, energy and metals industries and related businesses on best practices to combat illicit shipping and sanctions evasion practices, particularly regarding activities involving Iran, North Korea and Syria.

Among other things, the Advisory highlighted a number of methods used to facilitate illegal maritime trade or conduct. These red flags, requiring heightened due diligence, included:

- disabling or manipulating the AIS on vessels;
- physically altering vessel identification;
- falsifying cargo and vessel documents;
- STS transfers;
- voyage irregularities;
- false flags and flag hopping; and
- complex ownership or management structures.

Some of the best practices recommended to help effectively identify potential sanctions evasion included establishing AIS best practices. In particular, the Advisory recommended continuously broadcasting AIS locations, particularly in high-risk areas, and monitoring vessels to ensure continuous AIS broadcasting. The Advisory also indicated that consideration should be given to whether STS transfers were appropriate. Where undertaken, prior to the STS transfer, vessel operators should verify the other vessel's name, IMO number, and flag, and check that it was broadcasting AIS.

The Advisory also recommended that companies across the maritime supply chain review recipients and counterparties to a transaction to ensure the commodities being handled were not subject to sanctions. Companies were encouraged to review all the shipping documentation, including bills of lading that described cargo origin and destination and export licences where applicable, and other voyage details, based on the overall risk assessment of a

transaction's parties, vessel, cargo and route. While the Advisory was limited to making recommendations and providing guidance, it indicated that a failure to implement effective measures to avoid illegal activities (essentially overlooking red flags) could lead to regulatory scrutiny and sanctions.

Following on from this Advisory, in August 2021, the USCG updated its Cyber Strategic Outlook with a vision for protecting maritime transportation systems and operating safely in cyber space.

As to more general industry guidance, the International Maritime Organisation (IMO) published Guidelines of Maritime Cyber Risk Management in July 2017. These guidelines provided high-level recommendations on maritime cyber risk management to safeguard shipping from cyber threats and vulnerabilities. They also included functional elements that supported effective cyber risk management that could be incorporated into a vessel's existing risk management processes to complement the safety and security management practices already established by the IMO.

These guidelines were subsequently adopted by the IMO's Maritime Safety Committee through a Resolution on Maritime Cyber Risk Management in Safety Management Systems. This Resolution encouraged shipping organisations to ensure that cyber risks were appropriately addressed within a vessel's existing safety management systems, as defined in the International Safety Management (ISM) Code, in time for the vessel's next annual ISM Document of Compliance verification, after 1 January 2021. The ISM Code is the IMO's international code for the safe management and operation of ships at sea and became mandatory when it was incorporated by amendment into the IMO's International Convention for the Safety of Life at Sea (SOLAS) 1974.

In addition, international shipping organisation BIMCO has also produced Guidelines on Cyber Security Onboard Ships, the fourth and updated version of which was published in December 2020. These guidelines were prepared in conjunction with a number of other shipping organisations (including the International Chamber of Shipping) and they provide industry cyber risk management guidelines. Upon their publication, the chair of BIMCO's cybersecurity working group, Mr. Dirk Fry, highlighted that the maritime industry had been subjected in recent years to several significant incidents that had had a severe financial impact on the affected companies and that, with the increased connection of devices and systems to the internet, more opportunities would present themselves and more vulnerabilities in need of safeguarding would emerge in the future. The guidelines were intended to help address these concerns. BIMCO has also, in 2019, produced a cybersecurity clause that requires the parties to a charterparty to notify each other of any cybersecurity incident.

Some other industry guidance is also worth noting. In March 2020, the Digital Container Shipping Association published a Cyber Security Implementation Guide to assist its members in complying with the IMO requirements. In April 2020, the International Association of Classification Societies published their Recommendation on Cyber Resilience to help ensure standard criteria for newly built ships. The ship approval system Rightship has also introduced cyber risk security policies and procedures that are arguably more stringent than the IMO Guidelines.

More generally, the US National Institute of Standards and Technology (NIST) has usefully provided a Cybersecurity Framework composed of five key elements, namely: (1) identification of risk; (2) protection against cyberattack; (3) detection of cyber incidents; (4) response; and (5) recovery. The NIST Framework provides high-level best practice guidance that has been translated into many languages and is widely used, including by governments. While not industry-specific, it is a very useful tool to be used in conjunction with industry-specific guidance and regulation.

Legal Exposure

Cyber incidents that may lead to an involuntary breach of international sanctions could well result in the imposition of significant financial penalties and reputational damage.

More generally, cyberattacks do not only affect the party directly targeted. They can lead to third-party liabilities towards others who have been impacted. Issues may also arise as to whether the incident in question is covered by any insurance taken out.

In the shipping context, for example, if a ship's OT systems are hacked, this might lead to liabilities to the owners of cargo on board the ship if the cargo suffers damage or the vessel arrives late with cargo in a deteriorated condition. Alternatively, such a hacking incident might result in a collision with another ship, leading to liabilities towards that other ship. Furthermore, while a ship's protection and indemnity insurance cover might not contain a cyber-exclusion clause, such cover will normally provide that a ship must comply with all statutory requirements and maintain all valid certificates. A breach, for example, of the ISM cyber risk management requirements could arguably impact insurance coverage.

An organisation should, therefore, ensure that it has in place all necessary procedures and systems to demonstrate that it did all it could to ensure that it was cyber-secure. This later requirement of enhanced due diligence is now crucial in order to avoid arguments as to the unseaworthiness of the vessel and even the possibility that any right to limit liability could be lost in circumstances where it is shown that a failure to have in place adequate cyber defence amounts to recklessness.

The Regulatory Landscape

In May 2019, the EU issued a European Sanctions List for Cybercriminals and also adopted a regulation regarding restrictive measures against cyberattacks that threatened the EU or its Member States. The European Council has since extended this cybercrime sanctions framework twice, first until 18 May 2021 and then again until May 2022.

The EU cybercrime sanctions regime was partly prompted by a Russian military intelligence team's ultimately unsuccessful attempt to hack into the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Hague in 2018. Restrictions can include an EU travel ban, an asset freeze and a prohibition on making funds available to sanctioned entities. Sanctions may be imposed on individuals or entities regardless of nationality or jurisdiction, but only with the consent of all EU countries.

In July 2020, the EU imposed sanctions against six Chinese and Russian individuals and entities, as well as a North Korean entity, for their involvement in significant cyberattacks, or attempted cyberattacks, against the EU or its Member States. These cyberattacks included WannaCry, NotPetya, Operation Cloud Hopper and the cyberattack on OPCW mentioned above.

These sanctions were the first time that the EU had used its "cyber diplomacy toolbox" to impose sanctions against cyberattacks. The toolbox was established in June 2017 as part of the EU's Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities. The framework allowed the EU and its Member States to use various restrictive measures, including sanctions, to prevent and/or to deter cyberattacks against the EU.

In the UK, the Cyber (Sanctions) (EU Exit) Regulations 2020 were enacted to ensure sanctions aimed at furthering the prevention of certain cyber activity were implemented effectively after the UK left the EU. The Regulations were intended to have the same or similar effect as the EU Regulation.

With regard to the shipping industry specifically, shipowners and operators from signatory flag states must comply with the amendments to SOLAS relating to cyber risk management and the ISM Code, as discussed above.

Practical Problems

Cyber regulation is not of itself enough. Furthermore, being compliant and being cyber-secure are not necessarily one and the same thing. Shipping and other companies must have in place the relevant technology and appropriate procedures in order to control and minimise the risk.

Where the software used by shipping companies is not sufficiently robust, it is susceptible to cyber hacks that can involve the manipulation or theft of data. On board many ships, the original systems were installed before the risks of increasing connectivity were well known and the existing systems and networks may not be sufficiently protected against malicious cyber activity.

More modern ships may be even more exposed to cyber risk. Increased digitalisation means more connections, which mean more risk. More modern equipment on board ships will generally also retain larger amounts of data, which may be manipulated, misused or even lost. Therefore, the adverse consequences will be greater.

The IMO Guidelines identified a number of potentially vulnerable ship systems. Attention has also been drawn to specific threats for ships, such as the manipulation of AIS data, vulnerabilities in other satellite-based tracking systems, jamming global positioning systems (GPS), etc. Furthermore, even if the ship's Electronic Chart Display and Information System (ECDIS) is IMO-compliant, the technology is vulnerable to hackers and many systems are easy to tamper with.

Practical Solutions

Technology is a key factor in addressing cyber risk effectively. In this context, it is important to distinguish between information technology (IT) and operational technology (OT). In simple terms, IT systems control data. They might include email systems, electronic manuals and certificates, planned maintenance systems and so on. OT systems control equipment. Essentially, they comprise forms of hardware and software. In a maritime context, this could mean software/hardware that manages bridge navigation systems, machinery management systems, communication systems, cargo handling systems etc.

An attack on OT systems in a ship could impact the ship's operation or put at risk the crew's lives, or cause property or environmental damage. An attack on IT systems can lead to financial loss, reputational risk and legal disputes among other things. Furthermore and increasingly, IT and OT systems are integrated, with the consequence that a cyberattack can have more widespread ramifications than otherwise. This has been increasingly recognised within the maritime industry and, in fact, the IMO Guidelines recommend that a ship's cyber risk management plan should address risks to both systems and should put in place suitable pre-emptive measures against both types of risk.

There are a variety of technological measures that could help address cyber risk. Among other things: updating old systems and technology; investing in security tools such as firewalls, antivirus, content filtering, etc.; imposing authentication and authorisation procedures to limit system access; separating networks and critical systems insofar as possible; regularly monitoring and reviewing security measures for effectiveness, e.g. regular testing of systems and recovery plans, vulnerability assessment and so on.

Effective processes should also be in place. These could include procedures for backing up data and updating systems, as well as, policies on managing data; for example, regarding the encryption and retention of data (particularly sensitive data). In addition, regular software updates should be implemented by qualified persons. It may also be worth establishing best practice procedures for password use.

Employees should be made to understand that personal devices, including personal emails, should not be used for work-related communications. In addition, social media should not be used to share inappropriate work-related information. In the shipping context, shipowners and operators might introduce an appropriate procedure for ship-to-shore communications.

An effective procedure for managing incidents is also important. This may reduce the impact of an incident and restore systems as quickly as possible. It can also help to identify lessons learnt in order to avoid future similar incidents.

Employees should be given adequate training and support on how to identify cyber threats and how to deal with them, what to do if the IT/OT systems do not work and how to prevent cyber incidents. Having dedicated personnel tasked with being "cyber officers" may also be appropriate. Employees need not be cyber experts but they can, with the right support and training, develop an adequate grasp of how to avoid cyber incidents and how to address them if they arise. In simple terms, the running of "cyber drills" should be as common place as other regular ship's drills.

Innovation

Over the past few years, a large number of companies have offered effective cyber risk management services and advice on IT and OT governance. Some of these businesses offer support to companies generally, while others are more sector-specific in their offering. Additionally, there are associations, such as the UK's International Compliance Association (ICA), that offer education and training for the global regulatory and financial crime compliance community. The ICA has a number of global offices and members in 157 countries.

In shipping, a number of companies offer tailored maritime cybersecurity services. Others have gone one step further and offer an integrated cybersecurity solution for the maritime sector. One such example is InceMaritime. This is a collaboration between international law firm, Ince, with Mission Secure, one of the world's leading OT cybersecurity companies. Launched in February 2021, InceMaritime was the first initiative in the maritime industry offering integrated legal advisory, business consultancy and technology support.

In addition, in August 2021, InceMaritime Sanctions 2021 was launched. This is a collaboration between Ince, US law firm Seward and Kissel and Windward, a leading maritime predictive intelligence provider. This offering enables companies to access sanctions legal advice covering the UK, US and the EU, in conjunction with practical solutions such as high-level data analysis.

Other international law firms are now also embracing similar collaborations to address cyber risk in an integrated way. Undoubtedly, this is a business model that will be used increasingly in the future.

Conclusion

Advanced cyber technology has brought many benefits to the global economy but also many challenges. The challenges faced by the global maritime industry illustrate how cyber capability and cyber threat go hand in hand. The way in which cyber technology is being used as a tool covertly to breach international sanctions is a key example of the type of issues that can arise both in shipping but also more generally.

However, the regulatory and practical solutions that are highlighted above also demonstrate that the global shipping community, but also international businesses generally, are rising to the challenge and seeking to minimise the negative and enhance the positive in terms of cyber capability.

Julian Clark is the firm's Global Senior Partner with global responsibility for the firm's practice sectors and client base both in London and internationally. He is himself an internationally recognised leader in shipping and international trade with over 30 years' experience in mediation, arbitration and litigation. Julian has, for over 15 years, been ranked in the world's leading legal reference guides, including *Chambers and Partners 2020*, where he is described as being "recommended in the market for his strong relationship with P&I Clubs", *The Legal 500*, where he is ranked as a member of the Hall of Fame, the US publication *Super Lawyers*, and *Who's Who Legal*, who rank him as a "Global Leader".

Ince
Aldgate Tower, 2 Leman Street
London, E1 8QN
United Kingdom

Tel: +44 20 3823 7646
Email: JulianClark@incegd.com
URL: www.incegd.com

Reema Shour has been a professional support lawyer since 2009, having previously pursued a fee-earning career in shipping, trade and commodities, marine insurance and dispute resolution. Reema produces and co-edits the firm's external shipping and trade publications and has also contributed to various other external publications, including *Getting the Deal Through*, *World Arbitration Reporter* and *Chambers Shipping Guide*. She speaks five languages and works closely with the firm's global shipping, trade, marine insurance and dispute resolution teams, providing research, knowledge management, marketing and training support.

Ince
Aldgate Tower, 2 Leman Street
London, E1 8QN
United Kingdom

Tel: +44 20 7481 0010
Email: ReemaShour@incegd.com
URL: www.incegd.com

The Ince Group is a dynamic international legal and professional services business with offices in nine countries across Europe, Asia and the Middle East. With over 900 people, including over 100 partners worldwide, The Ince Group delivers legal advice, strategic guidance and business solutions to clients ranging from the world's oldest and biggest businesses operating across numerous industries to ultra-high-net-worth individuals. Through its entrepreneurial culture and "one firm" approach, the business offers its clients over 150 years of experience, insight and relationships. The Group is driven by a unique team of passionate people, whose broad expertise and deep sector specialisms provide their clients with solutions to all their complex legal and strategic needs.

www.incegd.com

Ince

Why AI is the Future of Cybersecurity


Akira Matsuda


Hiroki Fujita

Iwata Godo

Overview Surrounding Cybersecurity

What is cybersecurity?

Cybersecurity is defined as the "*preservation of confidentiality, integrity and availability of information in the Cyberspace*" in Article 4.20 of ISO/IEC 27032:2012.

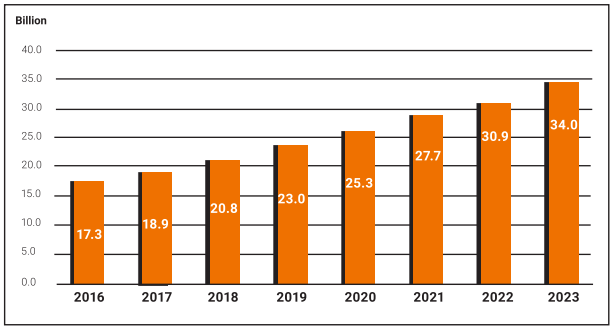
Furthermore, the cyberspace is defined as a "*complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form*" in Article 4.21 of ISO/IEC 27032:2012.

Threats in cyberspace

As internet access becomes more pervasive across the world and the Internet of things (IoT) devices become increasingly common and cyberspace expands rapidly, the number of cyber-attacks continues to grow. While an expanding cyberspace can be of great benefit to the public, the malicious use of cyberspace can result in significant economic and social losses. In cyberspace, cyber attackers have an asymmetric advantage over defenders. In particular, if defenders lag behind cyber attackers in terms of technology or defence systems, this advantage is likely to be enhanced. Unlike cyber attackers, it is difficult for defenders to introduce a new trial technology, because the defenders' main role is to ensure the stability of the defence systems that could be potentially harmed and undermined by the new trial technology.

Expansion of cyberspace

Along with technological development, cyberspace keeps growing. For example, there were globally 25.3 billion IoT devices active in cyberspace in 2020, and it is estimated that this number will reach about 34 billion by 2023.[1]



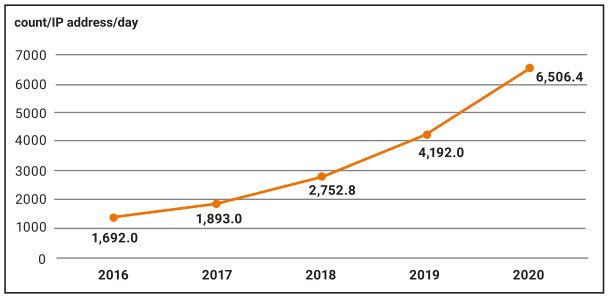
Note: the data is from "WHITE PAPER Information and Communications in Japan Year 2021" by the Ministry of Internal Affairs and Communications of Japan.

The governments of many countries share the view that digitalisation is transforming every aspect of our economies and societies. Data is increasingly becoming an important source of economic growth, and its effective use should contribute to social well-being around the world. In order to facilitate this process, the "Osaka Track" framework aimed at promoting international policy discussions and the drafting of international rules to enable the free movement of data across borders (international rules on trade-related aspects of electronic commerce at the World Trade Organization), with Japan intending to be a key player, was launched on 28 June 2019.

Threats in cyberspace

As cyberspace keeps growing, the frequency of cyber-attacks is increasing as a global trend. For example, in Japan, the number of unexpected connection attempts detected by the National Police Agency of Japan rose to 6,506 per IP address per day in 2020.

Number of unexpected connection attempts detected by the National Police Agency of Japan



Note: from "Threats in Cyberspace in 2020" by the National Police Agency of Japan.

New technologies and services, such as Artificial Intelligence (AI) and IoT, could bring about substantial benefits to the society of the future, as a society in which new values and services are created continuously, making people's lives more conformable and sustainable. On the other hand, there is a growing concern that these technologies could also be used in malicious ways. The risk is that users and providers of AI or IoT-related services will not be able to sufficiently and adequately control these technological developments and their use. With the growth of cyberspace, new threats are emerging and escalating and their scale, scope, and frequency increasing, as more sophisticated and organised attackers are designing targeted attacks to damage or disrupt critical infrastructures and services. These disruptions can have a huge financial impact or paralyse vital

activities. Cyber-attacks can generally lead to the loss of money, theft of personal information/identity/IP, to damage to reputation and safety, and cause problems with business services, transportation, health and power. For example, the largest oil pipeline in the U.S. was shut down for five days after a ransomware attack and paid a $4.4 million ransom to hackers in May 2021. In Japan, cyber-attacks were successfully conducted to steal crypto assets in 2018.

Superiority of cyber attackers

Cyberspace is a place where everyone can utilise new information and communication technology without being constrained by location and time. A cyber attacker has the decisive advantage as he can easily copy and disseminate data and information, including computer viruses/malware, and can flexibly use advanced technologies such as AI and blockchain. In contrast, it is generally difficult for defenders to respond to cyber-attacks because the resources they can use are limited, no defensive capability remains indefinitely effective and they are forced to respond with their then currently existing systems and technologies to ensure the stability and resilience of their defence system. Unlike cyber attackers, it is difficult for defenders to introduce a new trial technology because the new trial technology can harm or undermine the stability of defence systems. In addition, it is impossible to completely eliminate vulnerabilities caused by human errors linked to the use of information systems, so that many cyber-attacks involve looking for weaknesses in user behaviour that can be exploited through seemingly legitimate means (so-called "social hacking/social engineering").

Countermeasures

As cyber-attacks are spreading in cyberspace, where attackers seem to have a constant decisive advantage over defenders and their ability to assess and address risks, "Active Cyber Defense" can be considered to be an effective countermeasure to such cyber-attacks. Having an "Active Cyber Defense" means that the organisation proactively protects itself in advance rather than responding to a cyber-attack that has occurred. For example, the Ministry of Internal Affairs and Communications of Japan, which is the national watchdog in charge of cybersecurity-related laws and regulations, and the National Institute of Information and Communications Technology, which researches and promotes information and communications technology, have collaborated with internet service providers to launch the "NOTICE" programme designed to investigate IoT devices that might be misused/hacked in cyber-attacks because of weak authentification mechanisms (IDs and passwords), and to alert users. We understand that similar objectives are being pursued in many other countries.

The utilisation of AI is considered to be very important in organising an "Active Cyber Defense". This is because cyber attackers always use new offensive tools to conduct cyber-attacks, so that, in order to respond to cyber-attacks effectively, detection and analysis by AI are necessary. AI technology can be used to track new patterns or offensive strategies that could otherwise not be detected without machine learning mechanisms. In addition, by introducing AI in their defence strategy, humans can focus on their analysis of causes and impact at the time of a cyber-attack and, as the case may be react to, false detection. It is possible to increase the efficiency and accuracy of defence systems in cyberspace but to stay one step ahead is challenging.

Relationships Between Cybersecurity and AI

Trends/directions followed by AI utilisation

As for the direction of AI utilisation, as a general principle, there is a common understanding that it is extremely important not to excessively rely on AI and that humans should keep some control over the use of AI and AI-generated results and output. Ethics and morality would be negatively impacted by the excessive use of, and total dependence on, the use of AI. At this stage, many governments or integrated areas want to provide directions and guidance for the use of AI by issuing guidelines. For example, the "Principles for a Human-centric AI Society" were published in March 2019 in Japan and the "Ethics Guidelines for Trustworthy AI" were published by the European Commission in April 2019.

Relationships between cybersecurity and AI

The globally accepted and prevalent categorisation of the relationships between cybersecurity and AI is the following and can be divided into four categories: "Attacks using AI"; "Autonomous attacks by AI"; "Attacks against AI"; and "Security measures using AI".

Attacks using AI

Cyber attackers use AI for cyber-attacks. Such attacks are actually occurring in the real world.

Autonomous attacks by AI

AI performs cyber-attacks autonomously without human intervention. However, under the current AI model, this category is not yet in existence. Once it becomes technically possible for AI to perform cyber-attacks autonomously without human intervention, one difficulty will be to allocate responsibility for civil damage caused by cyber-attacks.

Attacks against AI

This category covers cyber-attacks against AI and the so-called "Adversarial Learning"; for example, where a cyber attacker may feed fake data to AI. Such an attack could become realistic in the future if human involvement in AI monitoring declines and the use of AI for critical decisions (such as medical diagnostics and investment decisions, etc.) becomes generalised.

Security measures using AI

This category covers defenders using AI against cyber-attacks. Various attempts have already been made, such as the automation of malware detection. At present, human beings continue to be responsible for determining those issues to be solved by AI and interpreting decisions by AI. Therefore, it is necessary to develop human resources that can fully utilise AI.

We discuss "Security measures using AI" in further detail below.

Security Measures Using AI

Benefits of using AI

There are four benefits of using AI for cybersecurity:

Reducing the cost of detection and response to breaches
Using AI for cybersecurity enables organisations to understand and reuse threat patterns to identify new threats. This leads to an overall reduction in time and effort to identify threats and incidents, investigate them, and remediate incidents.

Becoming faster at responding to breaches
A fast response is essential to protect an organisation from cyber-attacks. According to Capgemini's Reinventing Cybersecurity with Artificial Intelligence Report of 2019, using AI for cybersecurity, the overall time taken to detect threats and breaches is reduced by up to 12% and the time taken to remediate a breach or implement patches in response to an attack is also reduced by 12%. A small subset of organisations even managed to reduce these time metrics by more than 15%.

Increasing efficiency
Cyber analysts spend considerable time going through data logs and/or incident timesheets. Notwithstanding the significant workforce involved in cybersecurity, cyber analysts with deep knowledge of this field are rare. By using good data to analyse potential threats, AI enables cyber analysts to focus on work that only humans can do, such as analysing the incidents identified by the AI cybersecurity algorithms.

Making new revenue streams
As mentioned above, with the proliferation of IoT devices, the number, scope and scale of attacks have significantly increased. This creates opportunities for vendors offering cybersecurity services to manufacturers of IoT devices. Many players are taking advantage of the huge market opportunities.

Present Status of security measures using AI

As mentioned above, the benefits of using AI for cybersecurity purposes are plentiful but, at present, AI can only be used to assist human work conducted for the purpose of cybersecurity, and human involvement is necessary. In other words, it is still necessary for human beings to remain in charge of customising teacher data to be learned by AI, determining issues to be solved by AI, and interpreting AI decisions.

In addition, decisions by AI use the "black box" model that lacks transparency, providing only input-output without the underlying rationale, and it is difficult to determine why a decision has been made. In contrast, it is possible to clearly explain how white-box models behave and produce predictions and what the influencing variables are. However, they are yet to be put into practical use.

Security Measures Using AI and Fiduciary Duty of Care

Fiduciary duty of care

In many jurisdictions, directors and officers (hereinafter officers) of a company owe a fiduciary duty of care to the company. If an officer breaches a fiduciary duty of care in performing his/her role, the officer is liable to the company for the damage caused as a result.

Can it be considered that officers appropriately fulfil their fiduciary duty of care by introducing AI for cybersecurity purposes?

Use of AI for security measures and performance of fiduciary duty of care

As mentioned above, there are still many technical hurdles before AI can be used for security measures, so that the introduction of AI itself in corporate procedures and strategies does not necessarily mean that the officer in charge of cybersecurity is appropriately discharging his/her duty and can be exculpated if anything happens. Fairly common standards are used in many jurisdictions to determine the existence of a breach of fiduciary duty: whether the fiduciary duty of care is appropriately fulfilled is determined based on what would normally be expected from an ordinary officer having reasonable skills, experience and knowledge in a company of the same size and industry. Therefore, the introduction of AI does not necessarily mean that officers have appropriately fulfilled their fiduciary duty of care under the present state of the art where it is clear that adequate and sufficient cybersecurity protection cannot be achieved through the mere introduction of AI without appropriate human intervention and monitoring. Unless comprehensive security measures such as appropriate human intervention and human decision-making are introduced, cybersecurity measures could be deemed insufficient. Accordingly, it is important for officers to build comprehensive cybersecurity system frameworks, and AI could be used to achieve this purpose.

However, once these AI issues are resolved and the mere introduction of an AI-based cybersecurity system is widely recognised as appropriate for the cybersecurity protection of the company, it may be possible that an officer will be deemed to perform his fiduciary duty of care by simply introducing the appropriate AI-based cybersecurity system. If the absence of an AI-based cybersecurity system becomes a negative factor in the determination of a breach of fiduciary duty of care, it will be an incentive for all officers to introduce AI.

Future Prospects

As mentioned above, AI still has a lot of issues to overcome to form a stand-alone cybersecurity system. However, even at this early stage, in light of the benefits that could be derived from its use, AI will become an unavoidable tool in any efficient cyber defence strategy (especially where AI is being used in the attack).

Fortunately, the Tokyo Olympics and Paralympics were not interrupted by cyber-attacks, although the 2025 World Exposition to be held in Japan and the 2024 Paris Olympics and Paralympics are obvious targets. Major events have become attractive targets for "hacktivists" and fraudsters. The 2016 Rio de Janeiro Olympics and Paralympics and the 2018 Pyeongchang Winter Olympics and Paralympics have been under heavy attack (with allegations of cyberwarfare).

Cybersecurity is a hot topic and will be so for years to come. Every state, business and individual will need to remain wary and watchful: no doubt AI will help.

Endnote

1. The Ministry of Internal Affairs and Communications of Japan, "*WHITE PAPER Information and Communications in Japan Year 2021*", July 30th, 2021.

Akira Matsuda is an attorney-at-law (admitted in Japan and New York) and a partner at Iwata Godo heading the AI/TMT and Data Protection practice group. He is based in Tokyo and Singapore. His practice focuses on cross-border transactions, including mergers and acquisitions, as well as international disputes (litigation/arbitration), and advice on digital/TMT-related matters. Mr. Matsuda regularly advises Japanese and foreign clients on data security issues (Japanese laws, Singapore PDPA, and EU GDPR), including on the structuring of global compliance systems. He also advises complicated cross-border corporate investigation matters.
He is a graduate of the University of Tokyo (LL.B.) and Columbia Law School (LL.M.).

Iwata Godo
Marunouchi Building 15F
2-4-1 Marunouchi
Chiyoda-ku
Tokyo 100-6315
Japan

Tel: +81 3 3214 6205
Email: amatsuda@iwatagodo.com
URL: www.iwatagodo.com

Hiroki Fujita is an attorney-at-law (admitted in Japan) and associate at Iwata Godo. He is a member of the firm's AI/TMT and Data Protection practice group. His practice focuses on intellectual property law and IT. Mr. Fujita regularly advises clients across a broad range of industries, including electric power utilities and telecom carriers on data protection and cybersecurity issues. Mr. Fujita also advises clients on corporate matters, including mergers and acquisitions and corporate disputes (litigation/arbitration).
He is a graduate of Osaka University (LL.B.) and the Kyoto University School of Law (J.D.).

Iwata Godo
Marunouchi Building 15F
2-4-1 Marunouchi
Chiyoda-ku
Tokyo 100-6315
Japan

Tel: +81 3 3214 6205
Email: hiroki.fujita@iwatagodo.com
URL: www.iwatagodo.com

Iwata Godo is one of Japan's premier and oldest law firms. It was established in 1902 as one of the first business law firms by Chuzo Iwata, an attorney-at-law who subsequently held various positions, including serving as Minister of Justice and president of the Japan Federation of Bar Associations. It is a full-service firm with around 80 attorneys and each of its practice areas is highly regarded. It is the firm of choice for clients with respect to their most challenging legal issues, including in relation to data protection, privacy and cybersecurity.

www.iwatagodo.com

IWATA GODO
Established 1902

Australia


Dennis Miralis


Phillip Gibson


Jasmina Ceic

Nyman Gibson Miralis

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

In Australia, unauthorised access to computer systems is criminalised by both State and Federal legislation. In the Federal jurisdiction, hacking is criminalised under the *Criminal Code Act 1995* (Cth) ("*the Code*"). Most commonly, persons suspected of engaging in cybercrime are charged pursuant to *the Code*, given its universal application in all States and Territories in Australia.

Persons suspected of unauthorised access to computer systems are charged pursuant to s. 478.1 of *the Code*, which provides for the offence of "Unauthorised access to, or modification of, restricted data". The offence comprises three elements of proof. The offence is committed if: a person causes any unauthorised access to, or modification of, restricted data; the person intends to cause the access or modification; and the person knows that the access or modification is unauthorised. The maximum penalty for a contravention of s. 478.1 of *the Code* is two years' imprisonment. For the purposes of this offence, "restricted data" means data to which access is restricted by an access control system associated with a function of the computer.

As an example of state-based legislation criminalising hacking against private computer systems, Part 6 the *New South Wales Crimes Act 1900* ("*NSW Crimes Act*") – Computer Offences sets out multiple offences centred around unauthorised access, modification, or impairment of restricted data and electronic communications.

Denial-of-service attacks

Denial-of-Service attacks ("DoS attacks") or Distributed Denial-of-Service attacks ("DDoS attacks") are criminalised by s. 477.3 of *the Code*, which provides for the offence of "Unauthorised impairment of electronic communication".

The offence comprises two elements and is committed if a person causes any unauthorised impairment of electronic communication to or from a computer and the person knows that the impairment is unauthorised. The maximum penalty for a contravention of s. 477.3 of *the Code* is 10 years' imprisonment.

Phishing

Phishing, being a form of online fraud, is criminalised under *the Code* in instances where the victim is said to be a Commonwealth entity. When the victim is a member of the public, charges are brought under parallel State or Territory legislation. In New South Wales ("NSW"), charges could be brought under s. 192E of the *NSW Crimes Act*, which criminalises the general offence of fraud.

Prosecutions for Commonwealth fraud could encompass a wide variety of offending conduct, including phishing-style offences that would affect a Federal government body. Depending on the subsequent financial gain or loss suffered subsequent to the activity, the below charges are available:

- S. 134.2(1) – obtaining a financial advantage by deception.
- S. 135.1(1) – general dishonesty – obtaining a gain.
- S. 135.1(3) – general dishonesty – causing a loss.
- S. 135.1(5) – general dishonesty – causing a loss to another.

For the charge to be proven, the prosecution must establish that the accused obtains or causes a financial advantage, gain or loss by way of deception or dishonesty. The maximum penalty for each offence is 10 years' imprisonment.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

The infection of IT systems with malware is criminalised by s. 478.2 of *the Code*, which provides for the offence of "unauthorised impairment of data held on a computer disk etc.".

The offence comprises three elements and is committed if: a person causes any unauthorised impairment of the reliability, security or operation of data held on a computer disk, a credit card or another device used to store data by electronic means; the person intends to cause the impairment; and the person knows that the impairment is unauthorised. The maximum penalty is two years' imprisonment.

As an example of state-based offences of this nature, conduct of this type would likely be encompassed within the "modification or impairment" aspects of the *NSW Crimes Act* computer offences.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime is criminalised by s. 478.4 of *the Code*, which provides for the offence of producing, supplying or obtaining data with intent to commit a computer offence. The offence comprises two elements.

The offence is committed if: a person produces, supplies or obtains data; and the person does so with the intention that the data be used, by the person or another person, in committing an offence against Division 477 of *the Code* or facilitating the commission of such an offence. The maximum penalty for a contravention of s. 478.4 of *the Code* is three years' imprisonment.

Possession or use of hardware, software or other tools used to commit cybercrime
Possession or use of hardware, software or other tools used to commit cybercrime is criminalised by s. 478.3 of *the Code*, which provides for the offence of possession or control of data with intent to commit a computer offence.

The offence comprises two elements. The offence is committed if: a person has possession or control of data; and the person has that possession or control with the intention that the data be used, by the person or another person, in committing an offence against Division 477 of *the Code* or facilitating the commission of such an offence. The maximum penalty for a contravention of s. 478.3 of *the Code* is three years' imprisonment.

An example of a state equivalent can be found in ss 308F and 308G of the *NSW Crimes Act*.

Identity theft or identity fraud (e.g. in connection with access devices)
Identity crime, and in particular identity fraud offences, are criminalised by Division 372 of *the Code*. Particular acts that are criminalised include dealing in identification information, dealing in identification information that involves use of a carriage service, possession of identification information and possession of equipment used to make identification information. The offence of "Dealing in identification information that involves use of a carriage service" is most relevant to cybercrime. It is criminalised by s. 372.1A of *the Code* and comprises four elements. The offence is committed if: a person deals in identification information; the person does so using a carriage service; the person intends that any person will use the identification information to pretend to be, or to pass the user off as, another person (whether living, dead, real or fictitious) for the purpose of committing an offence or facilitating the commission of an offence; and the offence is an indictable offence against the law of the Commonwealth, an indictable offence against a law of a State or Territory or a foreign indictable offence. The maximum penalty is five years' imprisonment.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Electronic theft is criminalised by s. 478.1 of *the Code*. As the offence is committed if a person modifies restricted data, modification is defined in *the Code* as the alteration or removal of the data held in a computer, or an addition of the data held in a computer, the unauthorised copying of data from a computer would contravene the offence provision.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Penetration testing activity without authority could offend the above-mentioned s. 478.1 of *the Code*, which provides for the offence of "Unauthorised access to, or modification of, restricted data".

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Part 10.6 of *the Code* creates offences related to telecommunication services. They include offences relating to dishonesty with respect to carriage services and interference with telecommunications.

Additionally, the above-mentioned Part 6 of the *NSW Crimes Act* would likely be an example of state legislation that could cover these types of activities.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Extended geographical jurisdiction applies to offences under Part 10.7 of *the Code* (Divisions 477 and 478).

A person will not commit offences under that Part unless: the conduct constituting the alleged offence occurs wholly or partly in Australia, or wholly or partly on-board an Australian aircraft or an Australian ship; or the conduct constituting the alleged offences occurs wholly outside Australia and a result of the conduct occurs wholly or partly in Australia, or wholly or partly on-board an Australian aircraft or an Australian ship; or the conduct constituting the alleged offence occurs wholly outside Australia and at the time of the alleged offence, the person is an Australian citizen or at the time of the alleged offence, the person is a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory; or all of the following conditions are satisfied: the alleged offence is an ancillary offence; the conduct constituting the alleged offence occurs wholly outside Australia; and the conduct constituting the primary offence to which the ancillary offence relates, or a result of that conduct, occurs, or is intended by the person to occur, wholly or partly in Australia or wholly or partly on-board an Australian aircraft or an Australian ship.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

The *Crimes Act 1914* (Cth) prescribes the sentences applicable to breaches of Federal legislation, such as *the Code*. Relevant matters for consideration on sentences are set out as a non-exhaustive list of factors under s. 16A of the *NSW Crimes Act* (Cth). Matters that generally will mitigate a penalty include the timing of any guilty plea, the offender's character, the offender's prior record, assistance provided by the offender to the authorities and the offender's prospect of rehabilitation and likelihood of reoffending. The absence of intent to cause damage or make a financial gain could be taken into account by a sentencing court as a factor of mitigation.

A number of the offences particularised above cannot be "attempted"; they must actually be committed. For example, a person cannot attempt to commit the offence of "Unauthorised access, modification or impairment with intent to commit a serious offence".

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The following laws in Australia relate to cybersecurity: the *Privacy Act* (Cth) ("*Privacy Act*"); the *Crimes Act 1914* (Cth); the *Security of Critical Infrastructure Act 2018* (Cth); *the Code* (Cth); and the *Telecommunications (Interception and Access) Act 1979* (Cth).

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The *Security of Critical Infrastructure Act 2018* (Cth), which commenced on 11 July 2018, seeks to manage national security risks of sabotage, espionage and coercion posed by foreign entities. The Act was implemented as a response to technological changes that have increased cyber connectivity to critical infrastructure. The Australian Government considers "the responsibility for ensuring the continuity of operations and the provision of essential services to the Australian economy and community" as being shared "between owners and operators of critical infrastructure, state and territory governments and the Australian Government". The Act applies to approximately 165 specific assets in the electricity, gas, water and ports sectors.

The Act establishes a Register of Critical Infrastructure Assets, empowers the Secretary of the Department of Home Affairs with an information-gathering power (whereby certain information can be requested of direct interest holders, responsible entities and operators of critical infrastructure assets), and a Minister has the power to issue a direction to an owner or operator of critical infrastructure assets to mitigate national security risks.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The Australian Securities and Investments Commission ("ASIC") provides guidance to Australia's integrated corporate markets, financial services and consumer regulator, and organisations through its "cyber reliance good practices". The good practices recommend, *inter alia*, periodic review of cyber strategy by a board of directors, using cyber resilience as a management tool, for corporate governance to be responsive (i.e. keeping cybersecurity policies and procedures up to date), collaboration and information sharing, third-party risk management and implementing continuous monitoring systems.

The Office of the Australian Information Commissioner ("OAIC") recommends that entities have a data breach response plan that includes a strategy for containing, assessing and managing data breaches and strategies for containing and remediating data breaches.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

In February 2018, the *Privacy Amendment (Notifiable Data Breaches) Act 2017* amended the *Privacy Act* to require Australian Privacy Principles ("APP") entities to, as soon as practicable, provide notice to the OAIC and affected individuals of an "eligible data breach", where there are reasonable grounds to believe that an "eligible data breach" has occurred. This process is called the Notifiable Data Breaches Scheme ("NDB Scheme").

Eligible data breaches arise when: there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds; this unauthorised disclosure of personal information, or loss of personal information, is likely to result in serious harm to one or more individuals; and the entity has not been able to prevent the likely risk of serious harm with remedial action. Indicators such as malware signatures, observable network vulnerabilities and other "red-flag" technical characteristics may represent reasonable grounds for an APP entity to form a belief that an eligible data breach has occurred.

The OAIC expects APP entities to conduct a quick assessment of a suspected data breach to determine whether it is likely to result in serious harm.

The notification to the OAIC must include the identity and contact details of the organisation, a description of the data breach, the kinds of information concerned and recommendations about the steps that individuals should take in response to the data breach.

Under the *Privacy Act*, an APP entity is defined as an "agency" or "organisation". "Agency" includes a Minister, a department, and most government bodies, whilst "organisation" means an individual, a body corporate, a partnership, any other unincorporated association or a trust that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The affected individual must also be notified of an "eligible data breach", as defined above. The notification must include the identity and contact details of the organisation, a description of the data breach, the kinds of information concerned and recommendations about the steps that individuals should take in response to the data breach.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The OAIC is an independent statutory agency within the Attorney-General's Department. The OAIC has three functions; namely, privacy functions conferred by the *Privacy Act*, freedom of information functions, such as reviewing the decisions made by agencies and Ministers pursuant to the *Freedom of Information Act 1982* (Cth), and government information policy functions conferred by the *Australian Information Commissioner Act 2010* (Cth).

In relation to its privacy functions, the OAIC has the power to commence investigations, conduct privacy performance assessments, request an entity to develop an enforceable code, direct an agency to give the OAIC a privacy impact assessment about a proposed activity or function and recognise external dispute resolution schemes to handle privacy-related complaints.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

A failure to comply with the notification obligations can result in the imposition of substantial civil penalties. A serious or repeated interference with privacy attracts a fine of 2,000 penalty units, currently AUD 444,000.00. The maximum penalty that a court can order for a body corporate is five times the amount listed in the civil penalty provision, currently a maximum of AUD 2.1 million.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The *Privacy Act* confers a number of additional enforcement powers on the OAIC, including accepting an enforceable undertaking, bringing proceedings to enforce an enforceable undertaking, making a determination, making orders that the APP entity must redress any loss or damage suffered by the complainant and that the complainant is entitled to payment of compensation for such loss or damage, bringing proceedings to enforce a determination, delivering a report to the responsible Minister and seeking an injunction.

The OAIC reported that, in response to Commissioner-initiated investigations, enforceable undertakings were accepted by two APP entities during 2019, namely Wilson Asset Management (International) Pty Ltd, and the Commonwealth Bank of Australia.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There are presently no laws in Australia that prohibit the use of a Beacon or near-field communication technology.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There are presently no laws in Australia that prohibit the use of Honeypot technology or similar autonomous deception measures.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There are presently no laws in Australia that prohibit the use of Sinkhole technology. The malicious use of Sinkhole methods to steer legitimate traffic away from its intended recipient may, however, constitute an offence under s. 477.3 of *the Code*.

Sinkholes can be lawfully used as a defensive practice for research and in reaction to cyber-attacks. In this capacity, Sinkholes are a tool used by both public and private agencies.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

There are presently no laws in Australia that prohibit organisations from monitoring or intercepting electronic communications on their networks.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

There are presently no laws in Australia that prohibit the import or export of technology designed to prevent or mitigate the impact of cyber-attacks.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Market practice varies across different business sectors in NSW. The NDB Scheme, for example, only requires Australian government agencies, private sector companies and not-for-profit organisations with an annual turnover of more than AUD 3 million to report data breaches.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Part IIIA of the *Privacy Act* specifically regulates the handling of personal information about individuals' activities in relation to consumer credit, including the types of personal information that credit providers can disclose. All credit reporting bodies (defined in ss 6 and 6P as a business that involves collecting, holding,

using or disclosing personal information about individuals for the purposes of providing an entity with information about the creditworthiness of an individual) are subject to Part III.

Part 13 of the *Telecommunications Act 1997* (Cth) regulates carriers and carriage service providers in their use and disclosure of personal information. Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (Cth) requires providers of telecommunications services in Australia to collect and retain specific types of data for a minimum period of two years and must comply with the *Privacy Act* in relation to that data.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

A failure by a company to prevent, mitigate, manage or respond to an Incident may result in breaches of provisions of the *Corporations Act 2001* (Cth). The *Corporations Act 2001* (Cth) imposes duties on directors to exercise powers and duties with the care and diligence that a reasonable person would. A director who ignores the real possibility of an Incident may be liable for failing to exercise their duties with care and diligence.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Presently, the Applicable Laws do not require companies to designate a chief information security officer ("CISO"), establish a written Incident response plan or policy, conduct periodic cyber risk assessments or perform penetration tests or vulnerability assessments.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Other than those mentioned in section 2, no further specific disclosure is required in relation to cybersecurity risks or Incidents.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Australian common law does not recognise a general right of privacy. The equitable cause of action for breach of confidence may provide a remedy for invasions of privacy. Traditionally, the elements are that information must be confidential, information must have been imparted in circumstances importing an obligation of confidence and there must be an unauthorised use of that information. The current doctrine of breach of confidence does not currently entertain cases of wrongful intrusion, as opposed to cases of wrongful disclosure of confidential information.

The *Privacy Act* regulates the way Commonwealth agencies handle personal information. A person may obtain an injunction in the Federal Circuit Court against a Commonwealth agency that engages in, or proposes to engage in, conduct that is in breach of the *Privacy Act*. An action cannot be brought against an individual acting in their own capacity. A person may apply to the Court for an order that an entity pay compensation for loss or damage suffered by the person if a civil penalty has been made against the entity, or the entity is found guilty of an offence under the *Privacy Act*.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

No relevant civil proceedings or other private actions have been brought by individuals in relation to an Incident. Given the evolution of the doctrine of breach of confidence, it is likely such cases will be forthcoming.

Investigations conducted by the OAIC most commonly result in out-of-court outcomes. For example, a joint investigation conducted by the Australian Privacy Commissioner and the Privacy Commissioner of Canada into a highly publicised hacking breach of confidential data held by online adult dating service Ashley Madison resulted in an enforceable undertaking being entered into by the company pursuant to s. 33E of the *Privacy Act*.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

The High Court in *ABC v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 sanctioned the recognition of a tort of invasion of privacy. Judge Hampel in the case of *Doe v ABC* (2007) VCC 281 imposed liability in tort for the invasion of the plaintiff's privacy. Such reasoning may apply to an action in relation to a failure to prevent an Incident.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Organisations are permitted to take out insurance against Incidents in Australia. This includes breaches of the *Privacy Act*.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limits specifically targeted at losses associated with Incidents. Numerous entities offer insurance for data breaches, business interruptions, email forgery, ransomware attacks, costs of rebuilding an IT system, theft of crypto-currencies and legal fees associated with the investigation of Incidents. Coverage is governed generally by the *Insurance Act 1973* (Cth), the *Insurance Contracts Act 1984* (Cth), the *Corporations Act 2001* (Cth) and the common law.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

A number of well-established legal investigatory powers are deployed by law enforcement authorities when investigating an Incident. These powers can include the issuing of search warrants, the seizure of IT equipment for forensic analysis, decryption (whether at encrypted or decrypted data points) and the compulsory examination of suspects in certain circumstances.

The Australian Signals Directorate ("ASD") assumes responsibilities for defending Australia from global threats and advances its national interests through the provision of foreign signals intelligence, cybersecurity and offensive cyber operations as directed by the Australian Government. One of the express strategic objectives of the ASD is to provide advice and assistance to law enforcement. To this end, the ASD can collaborate with the Federal, State and Territory police forces in relation to matters of national interest, including emerging areas such as cyberterrorism.

See the answer to question 8.2 below for statutory notices that can be issued by law enforcement agencies to access data held by designated communications providers.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

On 8 December 2018, the Federal Parliament passed the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*. The Bill provides for the facilitation of covert access to data for the purposes of disrupting and investigating criminal activity, as well as establishing a framework to facilitate lawful assistance from communications providers.

The legislation allows various Australian law enforcement and intelligence agencies to make a Technical Assistance Notice ("TAN"), ordering designated communications providers to provide data or assistance in relation to criminal investigations or matters of security. This may include access to encryption keys or provision of decrypted data. Similarly, a Technical Capability Notice ("TCN") can be issued, mandating that a designated communications provider establish new capability to intercept and decrypt communications that would otherwise be encrypted or inaccessible.

The above notices may be issued in a broad variety of circumstances, including the enforcement of criminal laws and laws imposing pecuniary penalties, either in Australia or in a foreign country, or if it is in the interests of Australia's national security, Australia's foreign relations, or Australia's national economic wellbeing.

A designated communications provider, including an individual employed or acting on behalf of such providers, who has been compelled to provide data or assistance under a computer access warrant and fails to do so, may face up to 10 years' imprisonment, a fine of up to 600 penalty units (currently AUD 133,200.00) or both.

S. 3LA of the *Crimes Act 1914* (Cth) also provides law enforcement authorities a mechanism by which a person must provide information or assistance that is reasonable and necessary to allow a constable to: access data held in, or accessible from, a computer or data storage device that is on warrant premises or that has been moved to a place for examination under subsection 3K(2) of the *Crimes Act 1914* (Cth); copy data held in, or accessible from, a computer or storage device; and convert into documentary form, or another form intelligible to a constable, data held in, or accessible from, a computer or data storage device, or data held in a data storage device to which the data was copied, or data held in a data storage device removed from warrant premises under subsection 3L(1A) of the *Crimes Act 1914* (Cth).

Dennis Miralis is a leading Australian defence lawyer who specialises in international criminal law, with a focus on complex multi-jurisdictional regulatory investigations and prosecutions. His areas of expertise include cybercrime, global investigations, proceeds of crime, bribery and corruption, anti-money laundering, worldwide freezing orders, national security law, Interpol Red Notices, extradition and mutual legal assistance law. Dennis advises individuals and companies under investigation for economic crimes both locally and internationally. He has extensive experience in dealing with all major Australian and international investigative agencies.
Full biography: https://ngm.com.au/our-team/dennis-miralis-partner-defence-lawyer/.

Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: dm@ngm.com.au
URL: www.ngm.com.au

Phillip Gibson is one of Australia's leading criminal defence lawyers, with over 30 years of experience in all areas of criminal law. Phillip has significant experience in transnational cases across multiple jurisdictions, often involving: white-collar and corporate crime; asset forfeiture; money laundering and proceeds of crime; extradition; mutual legal assistance; Royal Commissions; bribery and corruption; and the Independent Commission Against Corruption ("ICAC") and Crime Commission matters. He has extensive experience in dealing with all major Australian and international investigative agencies.
Full biography: https://ngm.com.au/our-team/phillip-gibson-partner-specialist-defence-lawyer/.

Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: pg@ngm.com.au
URL: www.ngm.com.au

Jasmina Ceic is an accomplished criminal trial advocate. She advises and acts in complex criminal law matters at all levels of the court system, with a specialist focus on serious matters that proceed to trial in the Superior Courts, as well as conviction and sentence appeals heard in the Court of Criminal Appeal. She has represented and advised persons and companies being investigated for white-collar and corporate crime, complex international fraud and transnational money laundering.
Full biography: https://ngm.com.au/our-team/jasmina-ceic-senior-associate/.

Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: jc@ngm.com.au
URL: www.ngm.com.au

Nyman Gibson Miralis is an international award-winning criminal defence law firm based in Sydney, Australia. For over 50 years it has been leading the market in all aspects of general, complex and international crime, and is widely recognised for its involvement in some of Australia's most significant criminal cases.

Our international law practice focuses on cybercrime, white-collar and corporate crime, transnational financial crime, bribery and corruption, international money laundering, international asset freezing or forfeiture, extradition and mutual legal assistance law.

Nyman Gibson Miralis strategically advises and appears in matters where transnational cross-border investigations and prosecutions are being conducted in parallel jurisdictions, involving some of the largest law enforcement agencies and financial regulators worldwide.

Working with international partners, we have advised and acted in investigations involving the USA, Canada, the UK, the EU, China, Hong Kong, Singapore, Taiwan, Macao, Vietnam, Cambodia, Russia, Mexico, South Korea, the British Virgin Islands, New Zealand and South Africa.

www.ngm.com.au

NYMAN GIBSON MIRALIS
Criminal Defence Lawyers and Advisors est. 1966

Belgium


Roeland Lembrechts


Bart Van den Brande

Sirius Legal

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking, as an unauthorised access to an IT system, is criminalised under article 550*bis* of the Belgian Criminal Code (BCC).

The first distinction that must be made is between the basic crime (external and internal) and the subsequent actions.

External hacking happens when a person not possessing any access rights knowingly intrudes in or maintains access to an IT system. The penalties are between six months and two years of imprisonment and/or a fine of between 208 EUR and 200,000 EUR. In cases where a fraudulent purpose is found, the maximum imprisonment is increased to three years.

Internal hacking happens when a person, who has access rights, exceeds those rights with a fraudulent purpose or with the purpose of causing damage. The penalties are between six months and three years of imprisonment and/or a fine of between 208 EUR and 200,000 EUR.

Subsequent actions are aggravating circumstances with increased penalties: imprisonment of between one and five years; and/or a fine of between 208 EUR and 400,000 EUR. Subsequent actions can be stealing data, damaging an IT system or taking over an IT system to hack another system.

Instructing or commissioning a third party to commit hacking is punishable with between six months and five years of imprisonment and/or a fine of between 800 EUR and 1,600,000 EUR.

Knowingly disseminating or using data obtained as a result of hacking is punishable with imprisonment between six months and three years and/or a fine of between 208 EUR and 800,000 EUR.

Denial-of-service attacks
Denial-of-service attacks are criminalised as computer sabotage, i.e., "knowingly and without authorisation, directly or indirectly introducing, altering or deleting data in an IT system, or changing by any other technological means the normal use of any data in an IT system" (article 550*ter*, §1 BCC).

The penalties are between six months and three years of imprisonment and/or a fine of between 208 EUR and 200,000 EUR. If real damage is caused to the IT system, the maximum imprisonment is increased to five years and the maximum fine to 600,000 EUR.

In cases with a fraudulent purpose or intention of causing harm, the penalty is increased to a maximum of five years' imprisonment. The same increase applies to attacks against critical infrastructures.

Causing a disruption of the correct working of an IT system is an aggravating circumstance: penalties are increased to between one and five years' imprisonment and/or a fine of between 208 EUR and 800,000 EUR.

Phishing
This is, in most cases, punishable by article 504*quater* of the BCC, i.e., "with fraudulent purpose, acquiring an unlawful economic advantage for himself or for someone else, by introducing, modifying, deleting data that is stored, processed or transferred in an IT system, by means of an IT system or changing the normal use of data in an IT system by any other technological means".

The penalties are between six months and five years of imprisonment and/or a fine of between 208 EUR and 800,000 EUR. An attempt is punishable with six months to three years of imprisonment and/or a fine of between 208 EUR and 400,000 EUR.

Phishing may also be punishable under article 145, §3, 1° of the Electronic Communications Act of 13 June 2005 (ECA), prohibiting the fraudulent initiation of electronic communications, by means of an electronic communications network, with the intent to obtain an illegitimate economic advantage (for oneself or for another). This criminal offence is punishable with between one and four years of imprisonment and/or a fine of between 4,000 EUR and 400,000 EUR.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
This is an act of computer sabotage (article 550*ter*, §1 BCC).
The same criminal penalties apply as those applicable to denial-of-service attacks.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Article 550*bis*, §5 of the BCC provides a specific provision to penalise anyone who, unlawfully, imports, distributes, carries out or makes available in any way, any tool, including computer data, primarily designed or modified to enable hacking.
The penalties are between six months and three years of imprisonment and/or a fine of between 208 EUR and 800,000 EUR.

Possession or use of hardware, software or other tools used to commit cybercrime
It is a criminal offence on its own to illegitimately possess, produce, sell, procure for use, import, distribute, disseminate

or otherwise make available any instrument, including computer data, designed or adapted to enable hacking (article 550*bis*, §5 BCC) or computer sabotage (article 550*ter*, §4 BCC).

The penalties are between six months and three years of imprisonment and/or a fine of between 208 EUR and 800,000 EUR.

When this offence intercepts communication that is not publicly accessible, the penalties are between six months and two years of imprisonment and/or a fine of between 1,600 EUR and 80,000 EUR (article 314*bis*, §2*bis* BCC). If committed by a public officer, the penalties are between six months and three years of imprisonment and/or a fine of between 4,000 EUR and 160,000 EUR (article 259*bis*, §2*bis* BCC).

Identity theft or identity fraud (e.g. in connection with access devices)

Identity theft is often a precursor to another criminal offence, e.g., theft, fraud, computer fraud, hacking or computer sabotage committed by using the stolen identity.

Identity fraud may directly be a criminal offence only if the fraud relates to the appropriation of the capacity of a civil servant or military functions, nobility titles, the title of attorney-at-law or the public use of a false family name (articles 227–231 BCC). Penalties are usually limited to fines (up to 8,000 EUR).

Additionally, identity theft or fraud can be qualified as an illegitimate process of personal data. Depending on the specific qualification, these offences are punished by the Belgian GDPR Act of 30 July 2018 with a fine of between 2,000 EUR and 120,000 EUR (article 222), 800 EUR to 160,000 EUR (article 227) or 4,000 EUR to 240,000 EUR (article 223).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

There is no general qualification for electronic theft. Although there has been discussion, case law ruled that, e.g., theft of computer data can be punished under the general definition of theft (article 431 BCC).

As a subsequent action to theft, according to articles XI.304 and XV.105 of the Belgian Code of Economic Law, knowingly putting an unlawful copy of a computer program on the market or having it for commercial purposes, or putting on the market or having resources for commercial purposes that are exclusively intended for the unauthorised person to facilitate the removal or circumvention of technical provisions to protect a computer program, is punishable with imprisonment between one and five years.

Other intellectual properties are secured by articles XV.103–XV.106 of the Belgian Code of Economic Law with imprisonment between one and five years and/or a fine of between 4,000 EUR and 800,000 EUR in cases of infringement (piracy and counterfeit) with fraudulent and malicious purpose.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Unsolicited penetration testing is punished in the same way as hacking. It is sufficient that the hacker knows that he is not entitled to enter the IT system. The fact that there would be no damage or malicious intent is in principle irrelevant for criminalisation. Even the hacking attempt will be punished with the same penalties as a completed hacking.

Even with solicited penetration testing, the "white hat hacker" must be careful. The very broad moral element in the use and possession of hacker tools (article 550*bis*, §5 BCC) constitutes a criminal offence, even when they are used with the permission of the owner of the hacked IT system.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Article 210*bis* of the BCC punishes the committing of falsehood, i.e., "by entering data that are stored, processed or transferred through an IT system, into an IT system, to change, to delete or to change the possible use of data in an IT system with any other technological means, which changes the legal scope of such data".

The penalties are between six months and five years of imprisonment and/or a fine of between 208 EUR and 800,000 EUR.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Usually, there is no extraterritorial application of Belgian laws.

Article 3 of the BCC provides that the criminal courts shall be competent for all crimes in Belgian territory. To localise a criminal offence, Belgium applies the ubiquity doctrine, which provides that a criminal offence is situated in all places where there is a constitutive element to the offence.

This theory is supplemented with the principle of indivisibility, which allows courts to take into consideration all elements that are indivisibly connected with a criminal offence located in Belgium and to declare themselves competent with regard to a co-perpetrator located in a foreign country.

In the context of specific criminal offences, the Belgian criminal law provisions apply extraterritorially, e.g., in case of terrorism. The General Data Protection Regulation (GDPR) applies extraterritorially as per the criteria in article 3.2.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

A court may consider mitigating circumstances, such as the behaviour of the perpetrator, in determining the criminal sanctions or giving suspension/postponement of punishment. A pro-active notification or a declaration or plea of guilt may induce a court to impose lower penalties. An amicable settlement with the Public Prosecutor can also be possible.

Article 550*bis*, §1 has no reason not to criminalise ethical hacking. It is sufficient that the hacker knows that he is not entitled to enter the IT system. The fact that there would be no damage or malicious intent is in principle irrelevant for criminalisation. Even the hacking attempt will be punished with the same penalties as a completed hacking.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Cybersecurity:

- Act of 1 July 2011 on the security and protection of critical infrastructures.

- Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
- Act of 7 April 2019 establishing a framework for the security of network and information systems of general interest for public security.
- Royal Decree of 12 July 2019, implementing the law of 7 April 2019, establishing a framework for the security of network and information systems of general interest for public security and the law of 1 July 2011 on the security and protection of critical infrastructures.
- Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity), information and communications technology, cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
- Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for the application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems, and of the parameters for determining whether an Incident has a substantial impact.

Cybercrime:
- BCC, as amended by the Act of 28 November 2000 on cybercrime, and the Act of 15 May 2006 on cybercrime.
- Belgian Code of Criminal Proceedings.
- ECA.

Data protection:
- Article 22 of the Belgian Constitution.
- Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and the free movement of such data, and repealing Directive 95/46/EC (GDPR).
- Act of 3 December 2017 establishing the Data Protection Authority.
- Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data.
- Act of 5 September 2018 setting up the information security committee and amending various laws on the implementation of the General Data Protection Regulation and repealing Directive 95/46/EC.

Electronic communications, security of electronic communications and secrecy of electronic communications:
- Article 22 of the Belgian Constitution.
- Directive 2002/58/EC of 12 July 2002 on privacy and electronic communications.
- ECA.
- Articles 259*bis* and 314*bis* of the BCC.
- Coming soon: Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.

Trust services and electronic signatures:
- Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, and repealing Directive 1999/93/EC (eIDAS Regulation).
- Title 2 of Book XII of the Belgian Code of Economic Law.
- Act of 18 July 2017 on electronic identification.
- Act of 20 September 2018 on the harmonisation of the concepts of electronic signature and durable data carrier and the elimination of obstacles to the conclusion of contracts by electronic means.
- Royal Decree of 25 September 2018 on the harmonisation of the concepts of electronic signature and durable data carrier.

Intellectual property rights:
- Book XI of the Belgian Code of Economic Law.

Employee surveillance and BYOD:
- Article 22 of the Belgian Constitution.
- GDPR.
- ECA.
- Articles 259*bis* and 314*bis* of the BCC.
- Collective Bargaining Agreement No. 68 on employee camera surveillance.
- Collective Bargaining Agreement No. 81 on the protection of employees in relation to the surveillance of electronic online communication data.

Professional secrecy:
- Article 458 of the BCC.
- Act of 30 July 2018 on the protection of trade secrets.

Due diligence and due care:
- Articles 1382 and 1383 of the Belgian Civil Code.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Critical infrastructures are governed by the Critical Infrastructures Act (CIA). The personal scope of this Act is larger than that of Directive 2008/114/EC, which it implements in Belgian law. The CIA not only covers the energy and transportation sectors, but also the financial and electronic communications sectors.

There are no specific cybersecurity provisions in the CIA. It applies to all risks that may disrupt or destroy critical infrastructures, including cyber risks. Critical infrastructures must establish and execute a security plan, which may include cybersecurity measures.

The Belgian Cyber Security Act of 7 April 2019 (CSA) implements the NIS-Directive, applicable for operators of essential services and digital service providers. This Act provides a wide range of powers and means for the implementation, monitoring and sanctioning of obligations under the NIS-Directive, e.g., security plans, annual internal audits, triennial external audits and administrative and criminal sanctions.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Operators of essential services must take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems that they use in their operations, e.g., security plan, annual internal audit, triennial external audit, etc. (articles 20–23 CSA).

Digital service providers must identify and take appropriate and proportionate technical and organisational measures to

manage the risks posed to the security of their network and information systems. They shall take into account the following elements: (a) the security of systems and facilities; (b) Incident handling; (c) business continuity management; (d) monitoring, auditing and testing; and (e) compliance with international standards (articles 33–34 CSA).

Critical infrastructures must establish and implement a security plan (BPE) (article 13 CIA). This obligation implicitly includes Incident prevention and handling.

Providers of electronic communications services or electronic communications networks must implement adequate measures to manage the security risks in relation to their services or networks, including measures to mitigate the impact of security Incidents in relation to the end-users and other connected networks (article 114, §1 ECA).

Taking into account the state of the art, the controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (article 32 GDPR).

Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide (article 19 eIDAS Regulation).

The general principles of due diligence and due care will, in all likelihood, induce organisations to implement measures to prevent and handle Incidents in order to avoid or limit claims for damages. It does not, however, explicitly impose Incident prevention and handling.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Operators of essential services immediately report all Incidents that have a significant impact on the availability, confidentiality, integrity or authenticity of the network and information systems on which the essential service or services it provides depend on. This notification is simultaneously made to the national CSIRT, the sectoral government, or its sectoral CSIRT, and the Directorate General Crisis Centre of the Ministry of Interior Affairs.

The notification is required even if the operator only has partial access to the relevant information to determine whether the Incident has a significant impact (articles 24–25 CSA).

Digital service providers have the same duty for the services offered by them in the European Union. The notification is made in accordance with the implementing Regulation 2018/151 of 30 January 2018 on a secured platform (articles 35–36 CSA).

The controller under the GDPR shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Belgian Data Protection Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The notification must include the following information:

- the nature of the personal data breach;
- contact details of the data protection officer (DPO) or other contact point;
- the likely consequences of the personal data breach; and
- the measures taken or proposed to be taken.

Providers of electronic communications services/networks are subject to a binding personal data breach notification with the Belgian Data Protection Authority and, if impacted, the end-user, unless the provider has implemented mitigation measures (article 114/1, §3 ECA). They must also notify the Belgian Institute for Post and Telecommunications and the end-users about special security risks (article 114/1, §1 ECA). Security Incidents must also be notified to the Belgian Institute for Post and Telecommunications (article 114/1, §2 ECA).

Trust service providers must notify the Belgian Ministry of Economic Affairs or the Data Protection Authority about any breach of security or loss of integrity that has a significant impact on the trust service (article 19 eIDAS Regulation).

Critical infrastructures must notify any Incident that imperils the security of the critical infrastructure to the Communication and Information Centre (article 14, §1 CIA).

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Article 34 of the GDPR: When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate this breach to the data subject without undue delay. The information provided must, at least, include contact details of the DPO, likely consequences and measures taken or to be taken.

Article 114/1, §1 of the ECA: If there is a particular risk of network security breaches, the undertakings providing a publicly available electronic communications service shall inform subscribers and the Institute. If the risk requires measures other than those that can be taken by the undertakings providing the service, they shall indicate any means of combatting that risk, including an indication of the expected costs.

Article 19 of the eIDAS Regulation: When it is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall notify the natural or legal person of the breach of security or loss of integrity without undue delay.

The nature and scope of information is different for each notification duty.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The following regulators are responsible for enforcement (excluding criminal actions):

- Data protection: the Belgian Data Protection Authority.
- Electronic communications: the Belgian Institute for Post and Telecommunications.

- Trust services: the Ministry of Economic Affairs.
- Critical infrastructures: the Ministry of Interior Affairs.
- Operators of essential services and digital service providers: Centre for Cybersecurity Belgium (CCB), the Ministry of Economic Affairs and sectoral governments.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

The following penalties apply:

- Data protection: criminal penalties (indirectly to subsequent failures under article 226 of the Belgian GDPR Act) and administrative penalties (article 83, §4 GDPR).
- Electronic communications: criminal penalties (articles 114 and 145 ECA).
- Critical infrastructures: criminal penalties (article 26 CIA).
- Operators of essential services and digital service providers: criminal and administrative penalties (articles 51 and 52 Belgian CSA).

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

No specific information on enforcement is available. The focus is currently mainly on prevention and awareness with various government initiatives to increase maturity around cybersecurity. The data protection authority took its first series of decisions in 2020, including one decision with regard to taking adequate technical and organisational measures (decision 22/2020 of 8 May 2020). The authority ruled that there was no infringement as a Master IT Service Agreement had been concluded with the processor with the necessary provisions under GDPR, the necessary internal risk assessment methods had been taken, the effectiveness of the elaborated procedures had been evaluated by annual internal and external audits and the company acted in a transparent manner when reporting to the authority.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
This is not explicitly forbidden. It is only when the IP address is considered to be personal data under the GDPR that the processing must be compliant with the GDPR. An informed consent can be required in that case. Beacons, fingerprints and cookies also require informed consent under the ECA if they are not merely functional and/or collect personal data.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
This is not explicitly forbidden.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
This is not explicitly forbidden.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Organisations have a limited ability to intercept electronic communications, but in practice this is virtually impossible without committing a criminal act. Article 314*bis* of the BCC prohibits the deliberate interception, access or recording of communications in which one does not participate and without the consent of all participants. Article 124 of the ECA prohibits the deliberate knowledge of the existence of that communication, the identification of persons and the processing of the electronic communications that was obtained (deliberately or not) without the consent of all participants. Exceptions are provided for this last article, for example, Collective Bargaining Agreement No. 81, which provides for such an exception when necessary to prevent computers of the organisation from being hacked. However, the correct application is a subject of discussion in case law and legal doctrine.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

No, there is no explicit prohibition, except for the use of hacker tools, which is punishable by article 550*bis*, §5 of the BCC.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The market practice in relation to Incident handling varies greatly depending on the sector and nature of the activities.

Typically, the financial sector has implemented strict information security measures.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

The telecommunications sector is subject to specific obligations under the ECA (article 114/1).

Although these are technically not legal requirements, the financial services sector is subject to specific cybersecurity obligations in the context of the prudential supervision by the National Bank of Belgium.

In addition to this, the financial services sector and the telecommunications sector, together with the sectors of energy, transport, finance, healthcare, water and digital infrastructure, are governed by the CIA, which imposes security obligations.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

A director and/or officer may be held liable for a breach of his duties as a director if he fails to act with due care and due diligence.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

(a) There is no specific obligation to designate a CISO as such. Under the GDPR, it can be required to designate a DPO (article 37 GDPR). Operators of essential services and digital service providers are obliged to designate a contact point for the security of network and information systems (articles 23 and 34 CSA). The same obligation applies to critical infrastructures (articles 12 and 13 CIA).

(b) A written response plan or policy is required under articles 20 and 21 (operators of essential services) and article 33, §1, b) (digital service providers) of the CSA.
Article 13 of the CIA requires that the operator is responsible for organising exercises and for updating the security plan.
It may be required under the GDPR, depending on the company's individual context. This is the case under article 35, §7, d) of the GDPR when a data protection impact assessment is needed and may also be required as a general but implicit security measure under article 32 of the GDPR.

(c) The CSA explicitly requires an annual internal audit and a triennial external audit for operators of essential services (article 38, §1 and 2). Article 13, §6 of the CIA: The operator is responsible for organising exercises and for updating the BPE, based on the lessons learned from the exercises or from any change to the risk analysis. It may be required under the GDPR, depending on the company's individual context.

(d) *Idem* as (c).

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There are no other specific disclosure requirements for companies in relation to cybersecurity risks or Incidents. If cybersecurity risks or Incidents have a major financial impact, there is a disclosure requirement in relation to the financial impact (e.g., in the annual report). If they have an impact on personal data, there is a disclosure obligation to the Data Protection Authority.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

In the case of negligence, any person suffering damage may file an action to obtain compensation. That person is required to adduce evidence of the existence of negligence (which may be adduced by evidencing a breach of Applicable Laws), the damages suffered and the causal link between the negligence and the damage.

If the Incident is the result of an unfair market practice or a breach of data protection law, cease-and-desist proceedings are possible.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

Although there have been several Incidents, there have recently been no noteworthy cases in relation to Incidents.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes, see question 6.1.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Cyber insurance is permitted and even encouraged in Belgium.

The number of Incidents has even led to a greater general awareness and demand for insurance against Incidents.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are generally no legal or regulatory limitations in relation to insurance coverage, except the possibility for insurance against criminal penalties. Administrative fines may, however, be covered by insurance.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Law enforcement authorities have a variety of investigatory powers at their disposal, including:

- conducting (international) network searches;
- the right to copy, block or seize electronic data;
- intercepting, localising and accessing electronic communications;
- imposing technical cooperation from persons with knowledge about the relevant IT systems; and
- under very specific circumstances, hacking and computer sabotage, as well as decryption.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Organisations are not required to implement backdoors. However, law enforcement authorities may require any person with the relevant knowledge to provide them with encryption keys.

Roeland Lembrechts is a Master of Criminology (2005) and Master of Law (2009). He started his career in 2009 at the Bar of Mechelen with a broad focus on criminal, civil and corporate law, and specialised in contractual and non-contractual liabilities.
In addition, Roeland was an active as a board member of the department of contract law at the Bar of Antwerp (2018–2019) and is secretary of the professional journal *Today's Lawyer*, a magazine that focuses on the lawyer as an ethical and innovative entrepreneur with a focus on digitising the profession.
Roeland has a special interest in contract and liability law within the digital single market. He has been a certified DPO since 2017.

Sirius Legal
Veemarkt 70
2800 Mechelen
Belgium

Tel: +32 15 490 221
Email: roeland@siriuslegal.be
URL: www.siriuslegal.be

Bart Van den Brande has been a member of the Dutch-speaking Brussels Bar Association since 2001.
Bart has worked at several well-known Brussels law firms and has built extensive expertise in media and advertisement law, market practices and consumer protection, intellectual property, internet and e-commerce, privacy and data protection, IT, software development and gambling law.
Parallel to his law practice, Bart was a part-time teaching assistant at Brussels University VUB between 2005 and 2013. He is the author of several articles, is an experienced speaker at seminars and for training courses and is regularly asked to comment on current legal events in the national media. Several court cases handled by Bart were later published.

Sirius Legal
Veemarkt 70
2800 Mechelen
Belgium

Tel: +32 15 490 221
Email: bart@siriuslegal.be
URL: www.siriuslegal.be

Sirius Legal is a Belgian boutique law firm specialising in internet law, advertisement law, media and entertainment law, IP/IT, consumer protection, gambling and cybersecurity. The Sirius Legal team is a small and young but experienced team of law professionals that try to offer tailor-made solutions to a wide range of clients, ranging from multinationals to individual players.

www.siriuslegal.be

SIRIUS.LEGAL
BUSINESS LAW FIRM

Brazil


Fabio Ferreira Kujawski


Paula Moreira Indalecio


Paulo Marcos Rodrigues Brancher


Thiago Luís Sombra

Mattos Filho

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Federal Law No. 14.155/21 changed the description of the crime of invasion of electronic devices set forth in the Brazilian Penal Code. Article 154-A of the Penal Code prohibits the unauthorised access of computers and similar electronic devices to obtain, alter or destroy data, as well as the installation of vulnerabilities in such devices to obtain illicit benefits. The penalty ranges from one to four years of imprisonment, which could be augmented if the invasion results in access to private communication, commercial secrets, confidential information as established by law or the remote control of the tampered device, leading to a penalty of two to five years of imprisonment, as per §3º of article 154-A of the Penal Code. If the invading party divulges the data mentioned, or if the crime is committed against selected government officials, such as the President, Governors, Mayors, and others as listed by §5º of the same article, the penalty may be increased by a third. At the same time, §4-B and §4-C of article 155 of the Penal Code, altered by the referred federal law, determine the penalties of imprisonment, for four to eight years, if an individual commits theft through any electronic devices, which may or may not be connected to the internet, with or without the breach of security measures or usage of malicious programs.

Denial-of-service attacks
In addition to the applicability of article 154-A of the Penal Code, denial-of-service attacks may constitute the crime of terrorism if committed against public utility services, such as water or electricity distribution, airports, communication channels, hospitals, schools and stadiums, amongst other locations, in which case the agent is subject to a penalty from 12 to 30 years of imprisonment, as established in article 2 of Federal Law No. 13.260/16.

Phishing
Besides the modifications brought to article 154-A of the Penal Code, Federal Law No. 14.155/21 also added to the Penal Code the crime of electronic fraud, which qualifies as a type of fraud for the crime of embezzlement (set forth in article 171). In the legal text, §2-A establishes the penalties of imprisonment from four up to eight years, and a fine for frauds committed by misleading the victim through information received by social media, telephone contacts, the dissemination of fraudulent email or any other electronic fraud means. The penalties might increase by one-third up to two-thirds if the servers used to commit the fraud are not in the national territory, as stated by §2-B of the same article, or by one-third up to two times the baseline if the victim is elderly or vulnerable, as per §4º.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
The same considerations about articles 154-A and 155 of the Penal Code and article 10 of Federal Law No. 9.296/96 described in the "Hacking" section above should apply to any attempt to infect devices and systems with malicious programs.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
The first paragraph of article 154-A of the Penal Code prohibits the production, offering, distribution, sale, or diffusion of a device or computer program intended to be used to commit the crime listed in the head of the article, which is the unauthorised access of computers and similar electronic devices to obtain, alter or destroy data, as well as the installation of vulnerabilities in such devices to obtain illicit advantages.

Possession or use of hardware, software or other tools used to commit cybercrime
§1º of article 154-A of the Penal Code, only prohibits the production, offering, distribution, sale or diffusion of such tools, which means that the mere possession of such devices or their use in accordance with the law should not be considered a criminal offence.

Identity theft or identity fraud (e.g. in connection with access devices)
The Penal Code prohibits impersonation and identity theft through the use of electronic devices. Agents are subject to imprisonment of three months up to one year, or a fine. The State Court of Rio de Janeiro, by occasion of the judgment of civil appeal No. 0064038-07.2011.8.19.0042, ruled that creating an email to impersonate a known blogger could potentially characterise the crime of identity theft.

However, if the responsible party successfully misleads an individual and obtains illicit benefits, they could be charged for embezzlement, as per §2-A of article 171 of the Penal Code, mentioned under "Phishing" above.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
The same considerations about article 154-A and, particularly, article 155 of the Penal Code described under "Hacking" above

should apply if an individual commits theft through computer programs or other electronic means.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Even if the party responsible for the unsolicited testing fails at penetrating the IT system, the conduct may be considered an attempt to commit the crime established in article 154-A of the Penal Code. Other considerations about article 154-A of the Penal Code described in "Hacking" also apply here.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
The same considerations about article 154-A of the Penal Code described under "Hacking", and about article 2 of Federal Law No. 13.260 under "Denial-of-service attacks", apply if the activity in question fits the description of these articles.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Where crimes are committed on Brazilian soil or committed abroad, but the effects of said crimes occur in Brazil, they will be subject to the Brazilian law and jurisdiction.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

The penal legislation does not bring specific mitigating factors for cybercrimes but only aggravating ones. Nevertheless, all general mitigating factors available for other crimes apply to cybercrimes; for example, a crime committed for reasons of relevant social or moral value benefits may bring about mitigating factors.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

In 2018, the Brazilian Data Protection Law (Law No. 13,709/2018 – "LGPD") was sanctioned, and entered into force in August 2020. The LGPD establishes a new legal framework for personal data-processing operations and provides, among others, the rights of personal data subjects, the legal basis for data processing, and reporting obligations in case of data breaches. It also created the National Data Protection Authority ("ANPD").

The Brazilian Internet Act (Law No. 12,965/14) and Decree No. 8,771/16 govern certain security aspects for any online application.

For listed companies, the Brazilian Securities Commission's Resolution No. 35 establishes cybersecurity guidelines for broker entities, which cover cybersecurity policy, training for employees and risk assessment. Securities and Exchange Commission Ruling CVM/SEP 01/21 recommend that listed companies should include the cyber risks as a standalone risk factor in the company's annual reference form.

There are several sector-specific cybersecurity regulations, such as the financial services/banking (National Monetary Council's Resolution No. 4,893/2021), telecommunications (ANATEL Resolution No. 740/2020), medical devices (ANVISA Guide No. 38/2020), medical records (Federal Health Council Resolutions No. 1,821/2007 and 467/2020), insurance (Resolution SUSEP No. 638/2021), energy (ANEEL Resolutions No. 6,143/2019 and 6,197/2019).

As for the public sector, in February 2020, the Brazilian President approved the "National Cybersecurity Strategy" or "E-cyber", which provide general guidance and policies from the Federal Government during 2020–2023 (Decree No. 10.222/2020, National Cybersecurity Strategy/E-cyber).

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The sector-specific regulations explained in the preceding answer contemplate cyber policies that apply to critical infrastructure managed by their respective operators. In addition, Decree No. 10,569/2020 sets forth the National Strategy for Critical Infrastructure Security ("NSCIS"). The NSCIS seeks to determine strategic goals for the actions adopted by the Federal Government regarding critical infrastructure security in the public and private sector.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The LGPD requires organisations to adopt actions to prevent data incidents by employing technical and administrative measures suitable to protect personal data from unauthorised access and accidental or illicit destruction, loss, change, communication, or dissemination. Moreover, organisations must explain mitigating factors that may have been adopted in the context of reporting a data incident to the ANPD.

Most of the sector-specific cyber regulations cited in question 2.1 also impose similar obligations to their respective regulated entities.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

The LGPD provides that security incidents that could entail relevant risk or damage to the data subjects shall be communicated

to the ANPD and to the data subjects in a reasonable term, to be defined by the ANPD. The communication shall include: (i) a description of the nature of the personal data affected; (ii) information on data subjects involved; (iii) the technical and security measures used to protect personal data, respecting commercial and industrial secrecy; (iv) the risk related to the incident; (v) the reasons for a delayed disclosure, if the communication was not immediate; and (vi) the measures that were or will be adopted to reverse or mitigate the effects of the incident.

Sector-specific cyber rules also impose data breach reporting obligations to regulatory authorities.

Generally speaking, the communication shall include the description of the incident, the affected data categories; estimation on the number of data subjects potentially affected; measures adopted to mitigate the effects of the incident and the identified vulnerability; and duration of the vulnerability, among others.

When the incident is reportable to the ANPD, as a rule, it shall be reported to data subjects as well, as the law does not distinguish reporting obligations exclusively directed to the authority and to data subjects, as the GDPR does.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

As provided above, the LGPD provides that security incidents that could entail relevant risk or damage to the data subjects shall be communicated to the ANPD, as well as to the data subjects in a reasonable term, to be defined by the ANPD. The content of the communication shall be the same for both and is described above.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The ANPD is the government agency with technical autonomy but connected to the Cabinet of the Presidency, responsible for overseeing, issuing guidelines and enforcing the LGPD. Law No. 13,853/2019 expressly provides that ANPD has exclusive jurisdiction to enforce LGPD sanctions and, as far as protection of personal data is concerned, ANPD jurisdiction shall prevail over other public entities or organisations. Additionally, Decree No. 10,474/2020 regulates the governance structure of the ANPD and sets forth the responsibilities of the board of directors and other bodies that are part of the ANPD.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Non-compliance with the LGPD rules may result in the following administrative sanctions:

- a warning, with a specified deadline for the adoption of corrective measures;
- a one-time fine, of up to 2% of the turnover of a private legal entity, group, or conglomerate in Brazil in its preceding fiscal year, excluding taxes, limited to a total of 50 million Reais per violation;
- a daily fine, observing the total limit referred to in the previous point;
- public disclosure of the violation;
- blocking or elimination of the personal data impacted by the violation;
- partial suspension of the operation of the database not exceeding six months, extendable for an equal period, until the controller remedies the processing activity;
- suspension of the exercise of the processing activity of the personal data to which the violation refers for a maximum period of six months, extendable for an equal period; and
- partial or total prohibition of data processing.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

As mentioned in question 2.7 above, from a data protection perspective, the ANPD may apply some administrative sanctions, as provided in Section 52 of the LGPD. However, such sanctions only became effective as of August 2021 and, for this reason, we still do not have enforcement actions by the ANPD.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

There is no specific prohibition to use this measure to protect IT systems under the current law. However, please note that internet application providers are obliged to keep access logs from their users (including date, time and IP). The telecommunications network providers are forbidden to monitor or trace browsing information of their users, so this category of service providers should not make use of beacons.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

There is no specific prohibition to use this measure to protect IT systems under the current law. Notwithstanding, please note that honeypots may constitute interception of communication, which is a criminal offence under the Wiretap Act, when: (i) a third party listens to the communication of the caller and the intended call recipient without authorisation of such parties; and/or (ii) in the case of "covert listening", communication signals are captured through a transmitter stored at a physical location. Further information regarding this criminal offence is provided below at question 3.2.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)

There is no specific prohibition to use this measure to protect IT systems under the current law.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

The federal law that regulates the interception of communications is the Wiretap Act (Law No. 9296/1996). Article 10 of the Wiretap Act qualifies the "intercepting of telephone, computer or telematics communications, performing covert listening or breaking a secrecy of justice, without judicial permission or for purposes not authorised by law" as a criminal offence. Please note that the Wiretap Act does not lay out what qualifies as "interception" or "covert listening" – these concepts come from legal scholars/doctrine. In this regard, the caller and the intended call recipient are free to record communications to which they are a legitimate party and do not fall within the scope of "interception". This applies to employers that monitor calls and email traffic from their employees, to ensure compliance with cyber policies. We always recommend having corporate internal policies available to employees, where all processing operations and monitoring techniques are expressly disclosed to employees.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

No, there is no restriction for importing or exporting technology. There is one pending case at the Supreme Court that may rule on encryption matters and technical limits, in the context of law enforcement requests for content disclosure.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The LGPD is a comprehensive framework that establishes general principles and obligations relating to cybersecurity and protection of personal data that apply across multiple economic sectors and contractual relationships. Therefore, LGPD information security provisions apply to all business sectors. Notwithstanding, some sectors follow other specific security requirements as further described in the following answer.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Financial and Payments Institutions. There are cybersecurity regulations applicable to financial institutions, payment institutions and other entities authorised to operate by the Brazilian Central Bank ("BCB") that establish strict cybersecurity requirements, as well as specific requirements for engaging services of data processing and storage and cloud computing by the regulated entity, such as the Brazilian National Monetary Council's Resolution No. 4,893/2021, and the BCB's Resolution No. 85/2021. These rules are enforced by the BCB (for instance, by requesting that cybersecurity incidents are reported to BCB), and regulated entities may be subject to administrative sanctions in case of non-compliance with such rules. Financial sector and payment institutions also follow certain banking-specific security standards, such as PCI, but this is not a statutory requirement.

Internet connection and application providers. The Brazilian Civil Rights Framework for the Internet (Law No. 12,965/2014), alongside Decree No. 8,771/2016, which regulate the use of internet in Brazil, establish that internet connection and application providers shall, when retaining, storing and processing users' personal data or private communications, observe the following security guidelines: (i) strict control over access to the mentioned data; (ii) access authentication mechanisms, using, for example, double authentication systems to ensure the individualisation of the person responsible for processing data; and (iii) detailed inventory of access to internet connection and application records, containing the date, duration, identity of the employee or agent responsible for the access, appointed by the company, and the accessed file.

Capital Markets. The Securities and Exchange Commission ("CVM") has approved several regulations that establish information security requirements, requirements for contracting relevant third-party services and notification requirements in the event of a cybersecurity incident. Such rules are enforced by the CVM, which may impose sanctions in case of breach of the imposed requirements.

Telecommunications. The Brazilian Telecommunications Agency ("ANATEL") has also approved regulation on cybersecurity requirements applicable to telecommunications networks, critical telecom infrastructure and service platforms. Such regulation is enforced by ANATEL and regulated entities may be subject to administrative sanctions in case of non-compliance.

Public sector. The National Cybersecurity Strategy/E-cyber, approved in 2020, is a soft law that aims to guide federal government cyber actions for 2020–2023. The National Cybersecurity Strategy/E-cyber is not legally binding but is an important instrument to support the planning of government agencies and entities, whose objective was to improve the security and resilience of critical infrastructure and national public services.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

There is no specific rule imposing liabilities on directors or officers for a data incident, so the general liability of directors and officers for other types of violations shall apply. In this context, directors and officers should diligently manage the company's IT systems and ensure that the companies are adopting market standards for protecting their systems and applications. In case of breach of professional duties, directors and officers that are specifically in charge of the companies' systems and applications may be personally liable for the damages caused to third parties and to the company as a result of a data incident, when those directors and officers may have acted with recklessness, negligence or unskillfulness.

Please note that directors' and officers' insurance policies in Brazil offer coverage against directors' and officers' acts consisting of failures and non-compliance of data protection regulations stemming from management acts. The insurance coverage is available except in case of directors' and officers' wilful misconduct.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Generally, companies are not required to designate a chief information security officer ("CISO") or any equivalent position, but there are particular requirements for specific sectors.

Financial and Payments Institutions. Resolutions No. 4.893/2021 and 85/2021 issued by the Central Bank of Brazil ("BACEN") require financial and payment institutions to adopt cybersecurity policies and response plans. Notably, the Resolutions' requirements cover third-party service providers that contract with financial/payment institutions, including those located outside of Brazil. Under both Resolutions, financial/payment institutions are required to appoint an officer who will be responsible for implementing and overseeing the cybersecurity policy, and to adopt procedures and controls to prevent and respond to cybersecurity incidents.

Capital markets. CVM Instruction No. 505/2011 establishes rules and procedures to be observed in operations carried out in regulated securities markets. As part of the mechanisms and controls, the Instruction sets forth several information security requirements, including implementing a cybersecurity policy and guidelines for assessing the relevance of security incidents. Additionally, CVM Resolution No. 35/2021 establishes cybersecurity guidelines for broker entities, including cybersecurity policy, employee training and risk assessment.

Data Protection. The LGPD does not provide for specific security mechanisms but establishes that data-processing agents may adopt good practice standards and privacy governance programmes, which may include plans to respond to incidents and remediation, as well as cyber risk and vulnerability assessments. Even though the implementation of such standards and programmes is not mandatory under the LGPD, data-processing agents must adopt measures to prevent damages as a result of the data processing and must demonstrate the adoption of such measures, including their effectiveness. The ANPD will also consider the adoption of such standards and programmes when assessing the penalties to be imposed on companies in case of a data breach and/or non-compliance with the LGPD. Therefore, having an active cyber policy, training employees and conducting pen tests will certainly help mitigating sanctions that may be imposed by enforcement authorities.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Financial institutions are required to provide an annual report to the BACEN, disclosing any cybersecurity incidents as well as remediation efforts. Additionally, the CVM recommends that publicly held companies should include the cyber risks they face as a detailed risk factor in their annual reference form. In any event, should a data incident materially impact the companies' operations, assets and valuation, listed entities should disclose a relevant fact to the market.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Organisations involved in a security incident may face: (i) administrative proceedings initiated by consumer protection authorities; (ii) inquiries from the Public Prosecution Office; (iii) collective actions that may seek direct or moral damages filed by certain special categories of plaintiffs (including class associations and consumer protection entities); and (iv) individual claims in civil Courts.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

There are several actions brought in Brazil in relation to security incidents. Individuals frequently file civil actions for material and/or moral damages. Parts of the decisions state that individuals may only receive compensation for damages if they present evidence that their rights were violated and that the specific incident has caused damages. In several cases, the individuals attempt to apply the Consumer Code and the respective strict liability regime (where suppliers of services may be held liable irrespective of whether they acted with fault or negligence). Some Court decisions ruled in favour of the enforceability of the Consumer Code in the event of consumer data incident.

Other types of actions already filed in Brazil in the context of incidents require the controller to disclose the name of the data protection officer ("DPO") ("*Encarregado*"), provide more information about the incident, prove the adoption of data security and confidentiality measures, and resolve the vulnerability that has caused the incident. Such claims are commonly accepted by the Courts. Some cases specifically address the security incident as a failure of the service and/or a failure in the security systems of the controller, which is not always accepted by the Courts – in some cases, the incident is considered not directly related to the provision of the service by the provider or a failure in its systems. Some Courts rule that the risk of non-authorised use of personal data, without proof of actual damage, is a mere annoyance that does not necessarily trigger the controller's duty to indemnify.

Moreover, the Public Prosecutor's Office has filed civil actions in connection with data incidents. In one of the cases, an e-commerce platform user was commercialising personal data and was obliged to cease this action, even before the LGPD has entered into force. In another incident involving one of the main data brokers in Brazil, two of its products were prohibited. Other bodies of consumer national defence, as well as consumer defence institutes, have also filed civil actions, mostly against internet companies, for alleged unlawful processing. Other collective actions requiring the proper communication of the data breach to data subjects were also filed.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

As controllers have a duty to prevent data breaches, depending on the specific characteristics of a data incident, liability may arise out of controller's failure to adopt industry standard security mechanisms/technology.

The LGPD also contemplates certain events that may release controllers/processors from liability. So, processing agents shall not be liable when they prove that they did not perform the processing activity that caused the harm, when they prove that no violation of the data protection laws have occurred, or when the data subject or a third party was exclusively liable for the event.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to hire cyber policies in Brazil. The Superintendence of Private Insurance ("SUSEP"), the federal autarchy responsible for supervising the Brazilian insurance market, classified cyber risk insurance products as "comprehensive insurance", a regulatory type of product bundling several coverage modalities under the same policy. The SUSEP included cyber risk insurance products in the "liability" insurance segment through the SUSEP Letter No. 579/2018. The practice of the insurance industry in formatting and distributing these products follows the international experience, either through the establishment of first- and third-party coverage or by restricting the scope of coverage to risks arising from the use of technology in environments and that are not yet protected by other types of coverage.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Apart from the usual insurance coverage exclusions (e.g. acts of war, the insured's wilful misconduct, and non-compliance with the cybersecurity standards), claims on losses related to business interruption might face limitations to insurance coverage. Such limitations do not relate to expressed regulatory limitations but both normative and contractual interpretations.

Concerning the risk retention capacity of insurance companies authorised to operate in the country, a general limitation of a percentage of the adjusted net of the insurer for the underwriting of a sole risk applies. Insurers can accumulate additional risks by spreading them with other insurers or through reinsurance buying. Most cyber risk policies underwritten in Brazil have a coverage limit or cap, given that the extent of damages caused by a cyber-attack is difficult to estimate.

Regarding the regulation of contracts and policies for these products, the SUSEP maintains its liberalisation agenda and promotes the freedom to negotiate as its primary approach to products oversight. The SUSEP opted to leave cyber risk insurance contracts free of standard clauses.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Law enforcement has ample powers to conduct investigations according to the Brazilian Constitution and the Brazilian Code of Criminal Proceedings ("CPP"). Therefore, any legal orders given by the police must be obeyed, and refusal should entail charges of disobedience, as portrayed in article 330 of the Penal Code and mentioned in question 2.1 of this chapter. Law enforcement and prosecutors (which also have investigatory powers) can file requests seeking precautionary measures, which must always be authorised by a judge, such as the freezing of assets, search and seizure, temporary arrest, amongst several other measures for the investigation of cybercrimes.

Moreover, the LGPD provides specifically for the supervision and enforcement powers of the ANPD, which shall not only be notified of security incidents, but also may request further information regarding security incidents and apply relevant sanctions as the case may require.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no legal provisions of criminal nature compelling organisations to install backdoors in their IT systems. Nonetheless, there is one pending Supreme Court case involving a relevant messaging service provider that uses end-to-end encryption, thereby preventing the disclosure of message content to law enforcement authorities. The decision of this case will have an important effect on encryption technologies and access to decryption keys.

Fabio Ferreira Kujawski's practice focuses on technology, data protection and telecoms, with expertise in transactional and regulatory matters affecting these industries. He is considered a leading practitioner in his areas of expertise by several relevant legal directories (such as *Chambers and Partners* (Band 1 for Data Protection and Technology), *The Legal 500* and *Who's Who Legal*, among others). He is the co-author and editor of the book "*Legal Trends in Technology and Intellectual Property in Brazil*" (2014). He is an officer of the Brazilian Association of Information Technology and Telecommunications Law ("ABDTIC").

Mattos Filho
Alameda Joaquim Eugênio de Lima
447 – Jardim Paulista
São Paulo – SP, CEP 01403-001
Brazil

Tel: +55 11 3147 2795
Email: kujawski@mattosfilho.com.br
URL: www.mattosfilho.com.br

Paula Moreira Indalecio is a criminal lawyer with over 20 years' experience across various industry sectors. She works with both domestic and international clients on advisory and litigation matters concerning highly complex white-collar crime cases, particularly those involving technology and security-related issues. Since 2017, Paula has participated in annual discussion meetings at the Global Forum on Corporate Criminal Liability (organised by Cambridge Forums), becoming both a panellist and a member of the event's steering committee in 2019.

Mattos Filho
Alameda Joaquim Eugênio de Lima
447 – Jardim Paulista
São Paulo – SP, CEP 01403-001
Brazil

Tel: +55 11 3147 8588
Email: paula.indalecio@mattosfilho.com.br
URL: www.mattosfilho.com.br

Paulo Marcos Rodrigues Brancher's practice focuses on technology, IP and telecommunication, as well as antitrust, litigation and arbitration. He is a current member and co-director of the committee in data protection of ITechLaw, in which he acted for six years as a member of the management committee and three years as president of the membership committee for South America. He published several books, including issues related to software agreements, antitrust law and IP, and licensing agreements and IP.

Mattos Filho
Alameda Joaquim Eugênio de Lima
447 – Jardim Paulista
São Paulo – SP, CEP 01403-001
Brazil

Tel: +55 11 3147 4684
Email: pbrancher@mattosfilho.com.br
URL: www.mattosfilho.com.br

Thiago Luís Sombra's practice focuses on technology, compliance and public law, and, in particular, on anti-corruption investigations handled by public authorities and regulators, data protection, cybersecurity and digital platforms. He served as State Attorney of São Paulo before the Federal Supreme Court and Superior Court of Justice. He is currently a professor at the University of Brasília, member of the International Association of Privacy Professionals and the International Committee of Digital Economy of the International Chamber of Commerce.

Mattos Filho
SHS, Q 6 Conjunto A, Bl. C S. 1901
Brasília DF CEP 70316-109
Brazil

Tel: +55 61 3218 6010
Email: thiago.sombra@mattosfilho.com.br
URL: www.mattosfilho.com.br

Mattos Filho is structured to provide services to clients in different legal areas in a co-ordinated and integrated manner, working in multidisciplinary teams whenever necessary. This work dynamic allows the firm to deliver tailor-made solutions to its clients, thereby enhancing the understanding of their business and making it a valuable partner. Mattos Filho is a leader in approximately 30 different legal practice areas and works continuously to ensure that all these practices become benchmarks for the market. Creation of industry groups and market niches, combined with the firm's comprehensive knowledge of the market and clients' business needs, are examples of its efforts to keep it at the forefront in providing legal services. The firm represents domestic and foreign companies, financial institutions, investors, multilateral agencies, investment funds, pension funds, insurers and reinsurers and non-profit organisations.

www.mattosfilho.com.br

MATTOS FILHO >
Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados

Canada


Theo Ling


Andrew Chien


Ahmed Shafey


John Pirie

Baker & McKenzie LLP

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes, it is an offence to fraudulently obtain, use, control, access or intercept computer systems or functions under the *Criminal Code* (R.S.C., 1985, c. C-46). The relevant provisions of the *Criminal Code* that prohibit hacking (*i.e.*, unauthorised access) are as follows:

- Section 184: Any person who knowingly intercepts a private communication is guilty of an indictable offence carrying a maximum penalty of five years' imprisonment.
- Section 342.1: Any person who fraudulently obtains any computer services or intercepts any function of a computer system – directly or indirectly – or uses a computer system or computer password with the intent to do either of the foregoing, is guilty of an indictable offence carrying a maximum penalty of 10 years' imprisonment.
  - Recently, in *R. v. Senior*, 2021 ONSC 2729, the Ontario Superior Court summarised the essential elements required for the accused to be found guilty of an offence under Section 342.1 of the *Criminal Code*, and found the defendant guilty of unauthorised use of a computer after running a licence plate number contrary to York Regional Police directives.
- Section 380(1): Any person who defrauds another person of any property, money, valuable security or any service is guilty of: (i) an indictable offence carrying a maximum penalty of 14 years' imprisonment where the value of the subject matter of the offence exceeds $5,000; and (ii) an indictable offence or an offence punishable by summary conviction carrying a maximum penalty of two years' imprisonment where the value of the subject matter of the offence is under $5,000.
- Section 430: Any person who commits mischief to destroy or alter computer data; render computer data meaningless, useless or ineffective; obstruct, interrupt or interfere with the lawful use of computer data; or obstruct, interrupt or interfere with a person's lawful use of computer data who is entitled to access it, is guilty of: (i) an indictable offence punishable by imprisonment for life if the mischief causes actual danger to life; (ii) an indictable offence or an offence punishable on summary conviction carrying a maximum penalty of 10 years' imprisonment where the value of the subject matter of the offence exceeds $5,000; and (iii) an indictable offence or an offence punishable on summary conviction carrying a maximum penalty of two years' imprisonment where the value of the subject matter of the offence is under $5,000.
  - In *R. v. Geller*, [2003] O.J. No. 357, the accused was convicted under Section 430(5) after pleading guilty to "hacking" after obtaining 400 credit card numbers, along with other personal data, and accessing the internet 48 times using false identification.

Denial-of-service attacks

Yes. Under Section 430(1.1) of the *Criminal Code*, it is an offence to obstruct, interrupt or interfere with the lawful use of computer data or to deny access to computer data to a person who is entitled to access it; the maximum penalty for such an offence is 10 years' imprisonment.

Phishing

Yes. Phishing may constitute fraud under Section 380(1) of the *Criminal Code*. For example, in *R. v. Usifoh*, 2017 ONCJ 451, the accused was convicted of fraud relating to an email phishing scam emanating out of Nigeria and Dubai where he lured victims into sending funds. The maximum penalty for offences under Section 380(1) of the *Criminal Code* is 14 years' imprisonment.

In addition, while not a criminal offence, *Canada's anti-spam legislation* ("*CASL*") prohibits the sending of unsolicited commercial electronic messages ("CEMs"). Any person who contravenes *CASL* may be subject to an administrative monetary penalty of up to $1,000,000 in the case of an individual, and up to $10,000,000 in the case of any other person.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes. Under Section 430(1.1) of the *Criminal Code*, it is an offence to commit mischief in connection with computer data, as noted above. The maximum penalty for such an offence is 10 years' imprisonment; however, if a human life is endangered, offenders are liable to imprisonment for life.

In addition, Section 8(1) of *CASL* prohibits anyone in the course of a commercial activity, regardless of an expectation of profit, to: (i) install or cause to be installed a computer program on any other person's computer system; or (ii) cause an electronic message to be sent from that computer system, unless they receive the express consent of the computer system's owner or an authorised user, or if the person is acting in accordance with a court order.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

Yes. It is an offence under Section 342.2 of the *Criminal Code* to – without lawful excuse – sell or offer for sale a device that is

designed or adapted primarily to commit cybercrime, knowing that the device has been used or is intended to be used to commit a cybercrime that is prohibited under Sections 342.1 or 430 of the *Criminal Code* (described in more detail above).

The definition of "device" in Section 342.2 of the *Criminal Code* includes: (i) the component of a device; and (ii) a computer program (*i.e.*, computer data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function).

The maximum penalty under Section 342.2 is two years' imprisonment and/or forfeiture of any device relating to the offence.

Possession or use of hardware, software or other tools used to commit cybercrime

Yes. It is an offence under Section 342.2 of the *Criminal Code* to – without lawful excuse – possess, import, obtain for use, distribute, or make available a device that is designed or adapted primarily to commit cybercrime, knowing that the device has been used or is intended to be used to commit a cybercrime that is prohibited under Sections 342.1 or 430 of the *Criminal Code* (described in more detail above).

The maximum penalty is the same as noted above – *i.e.*, two years' imprisonment and/or forfeiture of any device relating to the offence.

Identity theft or identity fraud (e.g. in connection with access devices)

Yes. Sections 402.2 and 403 of the *Criminal Code* prohibit identity theft and identity fraud, respectively.

With respect to identity theft, it is an offence to obtain or possess another person's identity information with the intent to use it to commit an indictable offence like fraud, deceit, or falsehood. Furthermore, any person who transmits, makes available, distributes, sells or offers another person's identity information for the same purposes will be guilty of a criminal offence

Regarding identity fraud, it is an offence to fraudulently personate another person, living or dead, with the intent to: (i) gain advantage for themselves or another person; (ii) obtain any property or interest in any property; (iii) cause disadvantage to the person being personated or another person; or (iv) avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice.

Notably, the *Criminal Code* does not limit the aforementioned offences to any medium – *e.g.*, online, through access devices, or otherwise.

The maximum penalty for identity theft under Section 402.2 is five years' imprisonment, and the maximum penalty for identity fraud under Section 403 is 10 years' imprisonment.

In *R. v. Mackie*, 2014 ABCA 221, the accused pled guilty to 39 criminal charges, including three counts of identity fraud (and unauthorised use of a computer), after accessing the Facebook accounts of minors and personating those minors' friends to lure them into making child pornography.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Electronic theft is not specifically covered by the *Criminal Code*; however, depending on how the electronic theft is carried out and what is stolen, it may be considered an indictable offence under one of the many prohibitions against fraudulent transactions found in the *Criminal Code*. For example, any deceit, falsehood, or fraud by a current or former employee in order to knowingly obtain a trade secret, or communicate or make available a trade secret, is prohibited under Section 391(1) of the *Criminal Code*. And, similarly, it is an offence under Section 342.1 of the *Criminal Code* to fraudulently obtain any computer service, which includes data processing and the storage or retrieval of computer data.

In addition to the foregoing, Section 322 of the *Criminal Code* deals with theft generally. Many of the prohibitions in Section 322 against theft would cover electronic theft as well. For example, a person commits theft when he/she fraudulently and without colour of right takes or converts to his/her use anything with intent to deprive – temporarily or absolutely – the owner of his/her thing, property or interest therein. That said, the Supreme Court of Canada's historical approach to electronic theft is that non-tangible property, other than identity theft, is not considered property (see *R. v. Stewart*, [1988] 1 SCR 963) for the purposes of Section 322 of the *Criminal Code*. This interpretation has since been applied to data and images, which also cannot be the subject of theft under Section 322, although they can be the subject of other criminal offences (see, *e.g.*, *R. v. Maurer*, 2014 SKPC 118; *ORBCOMM Inc. v. Randy Taylor Professional Corp.*, 2017 ONSC 2308).

It is also a criminal offence to circumvent technological protection measures, or manufacture, import, distribute, offer for sale or rental, or provide technology, devices, or components for the purposes of circumventing technological protection measures under Section 41.1 of the *Copyright Act*. Knowingly circumventing technological protection measures for commercial purposes is a criminal offence under Section 42(3.1) of the *Copyright Act*, and can carry a maximum penalty of a $1,000,000 fine and/or five years' imprisonment.

Canadian privacy laws, including legislation relating to personal health information, also contain provisions prohibiting the unauthorised collection, use, disclosure and access to personal information ("PI"). For example, under Section 107 of Alberta's *Health Information Act*, RSA 2000, c. H-5, it is an offence to collect, gain, or attempt to gain access to personal health information in contravention of the Act (*e.g.*, by way of electronic theft without the authorisation of the relevant data subject); the maximum penalty for such an offence is a fine of $200,000 for individuals, and $1,000,000 for any other person.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Yes. Unsolicited penetration testing may be considered an offence under Section 342.1 of the *Criminal Code*. Under Section 342.1, individuals are prohibited from fraudulently, and without colour of right, obtaining, directly or indirectly, any computer service, or intercepting or causing to be intercepted, directly or indirectly, any function of a computer system. Unsolicited penetration testing may also be considered mischief under Section 430(1.1) of the *Criminal Code*.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Yes. Pursuant to Section 184 of the *Criminal Code*, it is an offence for any person to knowingly intercept a private communication, which is punishable by a maximum penalty of five years' imprisonment. Although the concept of "intercepting" generally requires the listening or recording of contemporaneous communication, in *R. v. TELUS Communications Co.*, [2013] 2 SCR 3, unlawful interception also applied to the seizing of text messages that are stored on a telecommunication provider's computer.

Moreover, under Section 83.2 of the *Criminal Code*, any person who commits an indictable offence under this or any other Act of Parliament for the benefit of, at the direction of or in association with a terrorist group is guilty of an indictable offence and liable to imprisonment for life. The definition of a "terrorist activity" under Section 83.01 includes an act that causes serious

interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of non-violent advocacy, protest, dissent or stoppage of work; this may include "cyberterrorism".

Under Section 19 of the *Information Security Act* (R.S.C., 1985, c. O-5), it is also an offence for any person to fraudulently, and without colour of right, communicate a trade secret to another person, or obtain, retain, alter or destroy a trade secret to the detriment of Canada's economic interests, international relations or national defence/national security. The maximum penalty under Section 19 is 10 years' imprisonment.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Section 6(2) of the *Criminal Code* states that "no person shall be convicted … of an offence committed outside Canada". That said, Canadian courts will exercise jurisdiction over an offence where there is a "real and substantial" link between that offence and Canada; a "real and substantial link" may exist where a significant portion of the activities constituting the offence occurred in Canada (see *R. v. Libman*, [1985] 2 SCR 178). Because cybercrime takes place online, the location of the server or computer is not always indicative of the location of the crime; therefore, the aforementioned offences may have extraterritorial application depending on the specific circumstances surrounding the relevant offence (*i.e.*, whether there is a "real and substantial link" to Canada).

Also, Section 26(1) of the *Security of Information Act* considers any person who commits an offence outside Canada to have committed the offence in Canada if the person is: (i) a Canadian citizen; (ii) a person who owes allegiance to Her Majesty in right of Canada; (iii) a person who is locally engaged and who performs his/her functions in a Canadian mission outside Canada; or (iv) a person who, after the time the offence is alleged to have been committed, is present in Canada.

Violations under *CASL* similarly have the potential for extraterritorial application. Section 12 of *CASL* applies to all CEMs accessed in Canada, including those sent from another country, and Section 8 prohibits the installation of computer programs without the express consent of the owner or authorised user of a computer system in Canada; this prohibition applies so long as the computer system is located in Canada.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

For criminal offences in Canada, there are no specific factors that would mitigate a penalty. Sentencing for criminal offences is assessed case by case, and Sections 718–718.21 of the *Criminal Code* provide guiding principles therefor. Some of the more relevant sentencing guidelines set out in the *Criminal Code* are outlined below.

- Section 718.1: "A sentence must be proportionate to the gravity of the offence and the degree of responsibility of the offender."
- Section 718.2(a): "A sentence should be increased or reduced to account for any relevant aggravating or mitigating circumstances relating to the offence or the offender."
- Section 718.21: This Section sets out a list of "additional factors" that courts will consider when imposing a sentence, including the "degree of planning involved in carrying out the offence and the duration and complexity of the offence".

There are also exceptions established under the *Copyright Act* that allow for circumvention of technological protection measures under certain circumstances. For example, Section 42(3.1) carves out any person acting on behalf of a library, archive or museum or educational institution from criminal liability for circumventing technological protection measures. Similarly, under Section 41.11, circumvention of technological protection measures is allowed for the purposes of national security.

Section 6 of *CASL* also provides for exceptions to the prohibition on unsolicited CEMs, including but not limited to messages that are sent by or on behalf of an individual to another individual with whom they have a personal or family relationship, or if the recipient of the communication has given express consent.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The *Criminal Code* prohibits the unauthorised use of a computer (Section 342.1), the possession of a device to obtain unauthorised use of computer system or to commit mischief (Section 342.2), and mischief in relation to computer data (Section 430(1.1)).

Section 19 of the *Security Information Act* and Section 391(1) of the *Criminal Code* also prohibit fraudulently obtaining or communicating a trade secret.

CASL protects consumers and businesses from the misuse of digital technology, including spam and other electronic threats, by prohibiting – in the course of commercial activity – (i) the alteration of transmission data in an electronic message so that the message is delivered to a destination other than or in addition to that specified by the sender (Section 7(1)), (ii) the installation of a computer program on any other person's computer system without express consent or court order (Section 8(1)), and (iii) the sending of a CEM to an electronic address in order to induce or aid any of the above (Section 9).

Sections 41 and 42 of the *Copyright Act* provide for civil and criminal remedies related to technological protection measures and rights management information.

There are various privacy statutes in Canada that regulate the way in which PI can be collected, used or disclosed:

- Canada's federal privacy legislation – the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*") – applies to private-sector organisations across Canada that collect, use or disclose PI in the course of commercial activity. Federally regulated organisations that conduct business in Canada are also subject to the PIPEDA, including their collection, use or disclosure of their employees' PI.
- Canada's federal government has proposed amendments in *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Act* ("*Digital Charter Implementation Act, 2020*"), which seeks to modernise the framework for the protection of personal information in the private sector.
- Alberta, British Columbia and Québec have their own private-sector privacy laws that have been deemed

substantially similar to the *PIPEDA*. Organisations subject to a substantially similar provincial privacy law are generally exempt from the *PIPEDA* with respect to the collection, use or disclosure of PI that occurs within that province.

- Québec has proposed significant potential amendments to its privacy laws in the public and private sector through Bill 64, *An Act to modernise legislative provisions as regards the protection of personal information*. These amendments require certain measures to be taken to protect confidential information stored in electronic documents and format, and set out rules governing the use, retention and transmission of electronic data.
- Ontario, New Brunswick, Nova Scotia and Newfoundland and Labrador have also adopted substantially similar legislation regarding the collection, use and disclosure of personal health information.

The *Telecommunications Act* (S.C. 1993, c. 38) also sets out regulations that telecommunications service providers must follow that may be applicable to cybersecurity.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Many departments and agencies across the Canadian government play a role with respect to cybersecurity in Canada for critical infrastructure and operators of essential services. All of these organisations engage with Public Safety Canada ("PS"); PS is the department responsible for ensuring coordination across all federal departments and agencies responsible for national security and the safety of Canadians and has released guidance on the fundamentals of cybersecurity for Canada's critical infrastructure community (see https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx).

Working with PS, the Communication Securities Establishment ("CSE") is the technical authority in Canada for cybersecurity and information assurance. Section 76 of the *Communications Security Establishment Act* (S.C. 2019, c. 13) ("*CSEA*") mandates the CSE to acquire, use and analyse information from the global information infrastructure, or from other sources, to provide advice, guidance and services to protect electronic information and information infrastructures. The CSE guides IT security specialists in the federal government through various IT security directives, practices and standards.

As part of its mandate, the CSE operates the Canadian Centre for Cyber Security and issues alerts and advisories on potential, imminent or actual cyber threats, vulnerabilities or incidents affecting Canada's critical infrastructure, which includes alerts on cyber threats to Canadian health organisations.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes. Organisations have an obligation under privacy laws in Canada to protect PI; an organisation's responsibilities include breach reporting, notification, and recording obligations in the event that an incident impacts PI.

For example, the PIPEDA requires organisations to protect PI by implementing security safeguards to protect against loss or theft thereof, as well as unauthorised access, disclosure, copying, use or modification. The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution and format of the information, and the method of storage. The methods of protection may include technological measures like using passwords and encryption.

Financial regulators in Canada also require or expect certain organisations to monitor, detect, prevent, or mitigate incidents, as detailed below:

- The Office of the Superintendent of Financial Institutions ("OSFI") issued an updated *Technology and Cyber Security Incident Reporting Advisory* document, which supports a coordinated and integrated approach to the OSFI's awareness of, and response to, technology and cybersecurity incidents at Federally Regulated Financial Institutions ("FRFIs").
- The Investment Industry Regulatory Organisation of Canada ("IIROC") provides various cybersecurity resources for Dealer Members to follow, including guides to help dealers protect themselves and their clients against cyber threats and attacks. The IIROC has also implemented rules for its Dealer Members to report cybersecurity incidents.
- The Canadian Securities Administrator ("CSA") issues cybersecurity-related staff notices, including: (i) CSA Staff Notice 11-326 (Cyber Security) to inform issuers, registrants and regulated entities on risks of cybercrime and steps to address these risks; (ii) CSA Staff Notice 11-338 (CSA Market Disruption Coordination Plan) to inform market participants about the CSA's coordination process to address a market disruption, including one that may stem from a large-scale cybersecurity incident; and (iii) CSA Staff Notice 33-321 (Cyber Security and Social Media) to inform firms on cybersecurity risks associated with social media use. Organisations regulated by the CSA are expected to conduct a cybersecurity risk assessment annually.
- The Mutual Fund Dealers Association of Canada ("MFDA") provides a Cybersecurity Assessment Program that offers mutual fund dealers assessments of their cybersecurity practices and advice on improving their defences. The MFDA released bulletins on cybersecurity to enhance member awareness and understanding of cybersecurity issues and resources and provide guidance regarding the development and implementation of cybersecurity procedures and controls.

In addition to the foregoing, the *Telecommunications Act* mandates telecommunications service providers to protect the privacy of their users through the provision of various consumer safeguards.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Organisations subject to the *PIPEDA* are required to report to the Office of the Privacy Commissioner of Canada ("OPC") any breaches of security safeguards involving PI that pose a real risk

of significant harm to individuals. The *PIPEDA* also requires organisations to keep records of any incident involving loss of unauthorised access to or unauthorised disclosure of PI due to a breach of (or failure to establish) the security safeguards required by the *PIPEDA*, and prescribes the minimum content for reports to the OPC, including but not limited to:

- a description of the incident;
- the timing of the incident;
- the PI impacted;
- an assessment of the risk of harm to individuals as a result of the breach;
- the number of individuals impacted;
- the steps to mitigate and/or reduce the risk of harm; and
- the name and contact information for a person at the organisation who can be contacted about the breach.

Similar breach reporting and notification requirements are found under other data protection statutes, including private-sector legislation in Alberta, public-sector legislation in the Northwest Territories and Nunavut, and legislation applicable to personal health information custodians in Ontario and Alberta.

Financial regulators such as the CSA, OSFI, IIROC, and MFDA also require the reporting of incidents. These incident reporting obligations generally pertain to any material systems issues, cybersecurity or technology risks and incidents, security breaches, breaches of client confidentiality or system intrusion.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The *PIPEDA* and Alberta's *Personal Information Protection Act* ("*PIPA*") require private-sector organisations to notify data subjects of certain breaches of their PI. Notification of data subjects might also be required or appropriate under provincial privacy laws. For example, provincial health privacy laws in Ontario, New Brunswick and Newfoundland and Labrador also have reporting requirements relating to the healthcare industry.

In particular, organisations subject to the *PIPEDA* are required to notify affected individuals about breaches of security safeguards involving PI that pose a real risk of significant harm to those individuals as soon as feasible. The notification must include enough information to allow the individual to understand the significance of the breach to them and to allow them to take steps, if any are possible, to reduce the risk of harm that could result from the breach. Other content and the manner of delivering the notice may be prescribed under the *PIPEDA* as well.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The Canadian Radio-television and Telecommunications Commission ("CRTC"), the OPC and the Competition Bureau are respectively mandated to enforce *CASL*, the *CASL*-related provisions of the *PIPEDA* and the *CASL*-related provisions of the *Competition Act* (R.S.C., 1985, c. C-34).

The OPC oversees compliance with the *PIPEDA*. There are certain offences under the *PIPEDA* that can be prosecuted by the Attorney General. Each provincial regulator is responsible for enforcing their provincial privacy statutes.

The Competition Bureau, an independent law enforcement agency, may also investigate false and misleading statements concerning consumers' privacy as a violation of the *Competition Act*.

See also the financial industry-specific regulators described in question 2.3, which regulate compliance with their industry-specific cybersecurity policies, guidelines and requirements.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

The OPC has the power to investigate complaints, audit and make non-binding recommendations in response to privacy violations. Upon the OPC's decision, an application can be made to the Federal Court for damages to complainants. The Attorney General can prosecute an organisation for failure to comply with the breach reporting, notification and recording obligations under the *PIPEDA*, which can result in fines of up to $10,000 on summary conviction or $100,000 for an indictable offence. Some of the provincial data protection statutes (*e.g.*, in British Columbia and Alberta) also provide for fines of up to $100,000 in the event of non-compliance.

The proposed *Digital Charter Implementation Act, 2020* – or any revised version thereof, if passed – may give the OPC new enforcement powers as well, including the ability to make binding orders and have the power to recommend fines to the new Personal Information and Data Protection Tribunal, established by the *Personal Information and Data Protection Tribunal Act* (not yet passed). This new privacy-focused tribunal would hear appeals from OPC orders and make decisions on whether to issue fines against organisations. Furthermore, the *Consumer Privacy Protection Act* (not yet passed) would allow the tribunal to impose fines of up to 3% of an organisation's gross global revenue or $10,000,000, whichever is higher. For more egregious offences, the Tribunal can issue fines of up to 5% of an organisation's gross global revenue or $25,000,000, whichever is higher.

Any organisation that makes false and misleading statements concerning consumers' privacy may also be subject to fines of up to $10,000,000 for a first offence and $15,000,000 for subsequent offences.

Penalties for criminal offences and non-compliance with *CASL* are described under question 1.1 (under "Phishing").

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The CRTC has taken enforcement action under *CASL* for violations of Sections 8 and 9, with fines of $100,000 to $150,000 for the unlawful distribution of advertisements through the offending parties' services.

The OPC regularly investigates incidents involving breaches of PI, including, for example:

- *PIPEDA* Findings #2021-001 – Joint investigation by federal and provincial privacy commissioners (Alberta, British Columbia and Québec) to examine whether Clearview AI, Inc.'s collection, use and disclosure of PI by means of its facial recognition tool complied with federal and provincial privacy laws applicable to the private sector.
- PIPEDA Findings #2020-005 – Investigation into Desjardins for a breach of security safeguards that affected close to 9.7 million individuals in Canada and abroad.
- PIPEDA Findings #2019-001 – Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with the *PIPEDA* regarding a breach of security safeguards resulting in the disclosure of PI in 2017.

- PIPEDA Findings #2016-005 – Investigation of Ashley Madison in connection with hacking and online posting of users' account information, which lead to OPC recommendations.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

Canadian privacy laws require users to provide consent to and/or be provided with sufficient notice of the collection, use and disclosure of their PI, and an opportunity to withdraw such consent.

The OPC's *Guidelines for identification and authentication* provide that because devices are usually associated with individuals, the metadata collected from devices through tracking mechanisms (*i.e.,* beacons) can be used to identify an individual without their knowledge. The metadata collected from such devices could include PI, the use of which may be considered surveillance or profiling. It is possible that certain exceptions under Canadian privacy laws may apply to the use of beacons (*i.e.*, Section 7(1)-(2) of the *PIPEDA*), and use thereof should be evaluated on a case-by-case basis.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

The use of honeypots is not expressly prohibited under applicable Canadian laws and, to our knowledge, there is currently no case law that provides further guidance. That said, the general application of Canadian privacy laws relating to the collection, use or disclosure of PI applies notwithstanding that they may be used defensively. The exceptions above relating to the use of beacons may also apply; however, such exceptions should also be evaluated on a case-by-case basis.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)

The use of sinkholes is not expressly prohibited under applicable Canadian laws and, to our knowledge, there is currently no case law that provides further guidance. That said, the general application of Canadian privacy laws relating to the collection, use or disclosure of PI applies notwithstanding that they may be used defensively. The exceptions above relating to the use of beacons and honeypots may also apply; however, such exceptions should also be evaluated on a case-by-case basis.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Employee monitoring is generally permissible under Canada's privacy legislation, but it must be carried out in compliance with such laws, and for a reasonable purpose, such as preventing, detecting, mitigating and responding to cyberattacks.

Privacy regulators use a reasonableness test set out in *Eastmond v. Canadian Pacific Railway*, 2004 FC 852, with regard to the collection of employee PI, which can be used in determining the reasonableness of a monitoring programme:

- Can it be demonstrated that monitoring is necessary to meet a specific need?
- Is the monitoring likely to be effective in meeting that need?
- Is any loss of privacy proportional to the benefit gained?
- Could the employer have met the need in a less privacy-invasive way?

Notification must be given for such a monitoring programme; for example, through an employee privacy policy. Monitoring employees in a unionised setting must be in compliance with applicable collective agreements and employee monitoring measures must comply with Canadian labour laws.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Canada has export controls in place to ensure that exports of certain goods and technology (*e.g.*, military and dual-use technologies) are consistent with national foreign and defence policies. The *Export and Import Permits Act* (R.S.C., 1985, c. E-19) authorises the Minister of Foreign Affairs to issue permits to export items included on the Export Control List or to a country included on the Area Control List, subject to certain terms and conditions. Factors impacting the need for a permit include the nature, characteristics, origin or destination of the goods or technology being exported.

The Department of Foreign Affairs, Trade and Development published a *Guide to Canada's Export Control List*, which addresses the trade of encryption items – *i.e.*, systems, equipment and components designed or modified to use cryptography for data confidentiality – under Category 5, Part 2: "Information Security". Due to its inclusion on the Export Control List, encryption or cryptographic technologies require an export permit such as the *General Export Permit No. 45 — Cryptography for the Development or Production of a Product* (SOR/2012-160).

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Market practices relating to information security usually do not vary substantially across business sectors. Certain sectors have supplementary information security requirements and/or recommendations (see question 4.2). Many organisations will also commit to a higher standard of information security beyond what is strictly required for compliance with sector-specific statutory requirements. For example, payment processors in Canada will usually choose to comply with the Payment Card Industry Data Security Standard ("PCI DSS"), a set of security standards overseen by an independent body, designed to ensure that organisations that accept, process, store or transmit credit card information maintain a secure environment.

The public sector also has specific information security requirements for all levels of government. For example, the *Privacy Act* (R.S.C. 1985, c. P-21) governs the PI-handling practices of federal government institutions and applies to all of

the PI that the federal government collects, uses and discloses. Canadian provinces, territories and municipalities have enacted similar legislation regulating the PI-handling practices of government institutions under their respective jurisdictions.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Yes, there are industry-specific requirements relating to cybersecurity in Canada.

Financial services providers must comply with federal and provincial laws that include specific provisions dealing with the protection of PI. For example, the Canadian *Bank Act* (S.C. 1991, c. 46) contains provisions regulating the use and disclosure of personal financial information and, through the enactment of regulations, may mandate Canadian banks to establish procedures for restricting the collection, retention, use and disclosure of personal financial information. Provincial laws governing credit unions also typically contain provisions dealing with the confidentiality of information relating to members' transactions. In addition, many provinces have laws that deal with consumer credit reporting, and these typically impose obligations on credit reporting agencies to ensure the accuracy and limit the disclosure of information. Financial service regulators have also published various recommendations relating to cybersecurity, including a series of guidelines developed by the Bank of Canada, Department of Finance and OSFI in collaboration with other G-7 partners.

Telecommunications service providers are also obligated to protect the privacy of their users by providing various consumer safeguards under the *Telecommunications Act*. The Canadian Security Telecommunications Advisory Committee ("CSTAC"), established to support Canada's National Strategy for Critical Infrastructure and Canada's Cyber Security Strategy, has published several guidance and best practice documents that telecommunications service providers should follow, including: (i) Security Best Practice Policy for CTSPs; (ii) Critical Infrastructure Protection Standard for CTSPs; (iii) Network Security Monitoring and Detection Standard for CTSPs; (iv) Security Incident Response Standard for CTSPs; and (v) Information Sharing, Reporting and Privacy Standard for CTSPs

Organisations in both the financial and telecommunication sectors must comply with the *PIPEDA*, including in relation to requirements regarding the PI of employees since business in both sectors is classified as a "federal work, undertaking or business".

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Under Canadian law, directors owe a fiduciary duty to their company to act in its best interests, and to exercise the care, diligence and skill that a reasonably prudent person would exercise in comparable circumstances, and can be liable for failing to satisfy such duty. These duties include an obligation to act prudently in the company's interests with regard to cybersecurity. Failure to take appropriate action to remedy known cybersecurity concerns that a reasonable person would have remedied could expose directors to personal liability. Directors and officers may also be exposed to personal liability for failures to adequately and truthfully represent an organisation's cybersecurity measures, or for failures to disclose cybersecurity incidents and risks.

In the event of a breach of duties, a due diligence defence may apply, where the director or office acted in good faith and at the guidance of professionals. For example, Section 54 of *CASL* sets out the due diligence defence for certain Sections of *CASL*, the *PIPEDA*, and the *Competition Act*.

Directors or officers may also be found personally liable under provincial privacy legislation as seen, by way of example, in Section 93 of Québec's *Act respecting the protection of personal information in the private sector*, C.Q.L.R c. P-39, and Section 64(2) of Manitoba's *Personal Health Information Act*, C.C.S.M. c. P33.5.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Under Canadian privacy laws (*e.g.*: Schedule 1, Principle 4.1 of the *PIPEDA*; Section 5 of Alberta's *PIPA*; and Section 4 of BC's *PIPA*), organisations are required to appoint an individual, or individuals, responsible for compliance with obligations under the respective statutes, including compliance with requirements relating to security safeguards. As Canadian privacy laws do not specify a particular title, these individuals may, for example, be referred to as the "Privacy Officer" or "Chief Information Security Officer".

Canadian privacy regulators have issued guidance documents, published findings and provided best practice recommendations for organisations to have established incident response plans and policies in place, conduct cyber risk assessments, and perform penetration tests/vulnerability assessments. While there is no strict requirement to abide by these guidance documents, failing to do so may result in non-compliance with an organisation's obligations under applicable privacy laws.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Section 45 of Québec's *Act to Establish a Legal Framework for Information Technology*, c. C-1.1, requires the disclosure of any creation of a database of biometric characteristics and measurements to the Commission d'accès à l'information.

Other laws within Canada may contain additional disclosure requirements, and organisations should confirm this on a case-by-case basis.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

An individual can enforce their rights by making a complaint to any of the privacy regulatory authorities mentioned in question 2.6 (or any other regulator discussed in this chapter). A

complaint may be made relating to an organisation's failure to comply with any of its statutory obligations to collect, use and disclose personal information in accordance with the principles of fair information practices set out in Canada's privacy legislation:

- accountability;
- identifying purpose;
- consent;
- limiting collection;
- limiting use, disclosure and retention;
- accuracy;
- safeguards;
- openness;
- individual access; and
- challenging compliance.

These authorities are generally required to investigate any such complaint.

Under the *PIPEDA*, a formal complaint must be investigated, and the OPC will issue a report outlining the findings of the investigation and any recommendations for compliance. The report may be made public at the discretion of the OPC. The complainant, but not the organisation subject to the complaint, may appeal to the Federal Court. The Court has broad authority, including the authority to order a correction of the organisation's practices, and award monetary damages.

Under Alberta's *PIPA* and BC's *PIPA*, an investigation may be elevated to a formal inquiry by the Commissioner and result in an order. Organisations are required to comply with the order, or apply for judicial review, within a prescribed time period. Similarly, under Québec's *PIPA*, an order must be obeyed within a prescribed time period. An individual may appeal to a judge of the Court of Québec on questions of law or jurisdiction with respect to a final decision.

Additionally, class action lawsuits may be filed in Canada in the aftermath of an incident that results in the breach of personal information. The most common causes of action advanced in class actions are:

- breach of confidence;
- breach of contract;
- breach of fiduciary duty;
- breach of Section 7 of the Canadian Charter of Rights and Freedoms;
- breach of the *PIPEDA* or the *Privacy Act*;
- breach of provincial privacy legislation;
- invasion of privacy:
  - intrusion on seclusion; and
  - publicity to private life (public disclosure of embarrassing private facts);
- negligence; and
- unjust enrichment.

The invasion of privacy torts is relatively new in the Canadian legal landscape. The tort of intrusion on seclusion was recognised in the Ontario Court of Appeal case *Jones v. Tsige*, 2012 ONCA 32. The tort of public disclosure of embarrassing private facts was recognised by the Ontario Superior Court in *Jane Doe 464533 v. ND (Jane Doe)*, 2016 ONSC 541.

The legal test for the tort of intrusion on seclusion requires objective proof that the alleged invasion of privacy would be highly offensive to a reasonable person.

The legal test for the tort of public disclosure of private facts requires proof that the matter publicised (the private facts) or was an act of publication: (a) would be highly offensive to a reasonable person; and (b) is not of legitimate concern to the public.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

In *Chitrakar v. Bell TV*, 2013 FC 1103, the Federal Court awarded the plaintiff over $20,000 in damages following a privacy violation by Bell TV, a telecommunications company. The Court held that Bell had failed to comply with its obligations pursuant to the *PIPEDA* by conducting a credit check without the plaintiff's prior consent. Prior to this decision, the federal Privacy Commissioner had found that the plaintiff's privacy rights were violated under the *PIPEDA*.

In *Karasik v. Yahoo! Inc.*, 2021 ONSC 1063, the Ontario Superior Court approved a class action settlement against Yahoo! relating to cyberattacks against Yahoo! by unidentified attackers that resulted in the exposure of personal information of 5 million Canadians. The certified issues for settlement included negligence in failing to take reasonable steps to establish, maintain, and enforce appropriate security safeguards, and negligence in failing to notify the Class Members about the incidents. In this decision, the Court undertook a deep analysis of the state of law for privacy class actions. The decision reflects the fact that while most privacy related class action cases are certified, none have gone to trial and *per capita* settlement amounts tend to be extremely low. As noted by the Court, "it will take a trial decision awarding more than notional-nominal general damages" to change the landscape.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes. In past class action lawsuits, representative plaintiffs have alleged various torts, including negligence in failing to prevent an incident. There have been no trial determinations for privacy class actions in Canada, though settlement approval decisions suggest that grounds exist to award damages on this basis.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against incidents. Many commercial insurers offer specialised cybersecurity insurance. This can be in the form of third-party liability coverage or first-party expense coverage, or both.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limitations.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Canada's Privacy Commissioners have broad powers under privacy statutes to investigate complaints, issue reports, compel

the production of evidence, issue monetary penalties and make recommendations or initiate audits.

Similarly, the CRTC has a broad range of investigative powers available under *CASL*. In addition to issuing monetary penalties, it may execute search warrants and seize items, as well as obtain injunctions (with judicial authorisation) against suspected offenders.

Local police, provincial police, and the Royal Canadian Mounted Police, along with the national security apparatus (*e.g.*, the CSE and the Canadian Security Intelligence Service) all have broad powers to investigate criminal activities relating to cybersecurity, including terrorism offences.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No. However, all of Canada's privacy statutes permit an organisation to disclose personal information without consent, where the disclosure is to a law enforcement agency in Canada and concerns an offence under Canadian law.

Under Québec's *PIPA*, an organisation may refuse to communicate personal information to the person in respect of whom the information relates, where such disclosure would be likely to hinder an investigation in connection to a crime or a statutory offence, or affect judicial proceedings in which the person has an interest.

Pursuant Section 27(2) of the *CSEA*, the CSE may be authorised by the designated federal minister to access any non-federal infrastructure that is of importance to the government of Canada, and acquire any information originating from, directed to, stored on or being transmitted on or through that infrastructure for the purpose of helping to protect it, in the circumstances described in paragraph 184(2)(e) of the *Criminal Code*, from mischief, unauthorised use or disruption.

Theo Ling is a partner in Baker McKenzie's Intellectual Property & Technology Practice Group. Theo's practice is focused on data and technology-related issues, and digital transformation and data governance initiatives that involve data privacy, data security, electronic payments, data monetisation, records retention, media/format, electronic signatures, cross-border data transfers, digitisation, fintech, and AI and machine learning considerations. Theo also advises clients on internet-related services that involve smart/connected devices, which are subject to regulation under telecommunications and broadcasting laws.

Baker & McKenzie LLP
181 Bay Street, Suite 2100
Toronto, Ontario, M5J 2T3
Canada

Tel: +1 416 865 6954
Fax: +1 416 863 6275
Email: theodore.ling@bakermckenzie.com
URL: www.bakermckenzie.com

Andrew Chien is an associate in Baker McKenzie's Intellectual Property & Technology Practice Group in Canada, and has over five years of experience advising multinational clients on complex intellectual property, data privacy, and other technology-related commercial and regulatory issues. Andrew provides practical advice to his clients in the context of cross-border transactions; business-to-business commercial relationships and agreements; data privacy and other information technology-focused compliance; and intellectual property protection strategies. Andrew also advises clients on related dispute resolution and enforcement matters that arise from these areas.

Baker & McKenzie LLP
181 Bay Street, Suite 2100
Toronto, Ontario, M5J 2T3
Canada

Tel: +1 416 865 2315
Fax: +1 416 863 6275
Email: andrew.chien@bakermckenzie.com
URL: www.bakermckenzie.com

Ahmed Shafey is a partner in Baker McKenzie's Litigation and Government Enforcement Practice Group in Canada. Ahmed is known for his focused and practical advice and has had success at all levels of the Court in Ontario as well as with a number of Boards and Tribunals. Ahmed is engaged by clients in a wide range of industries to provide advice in relation to cybersecurity- and data privacy-related concerns and is actively involved in a number of the Firm's innovations in the practice of law.

Baker & McKenzie LLP
181 Bay Street, Suite 2100
Toronto, Ontario, M5J 2T3
Canada

Tel: +1 416 865 6964
Fax: +1 416 863 6275
Email: ahmed.shafey@bakermckenzie.com
URL: www.bakermckenzie.com

John Pirie is a partner in Baker McKenzie's Litigation and Government Enforcement Practice Group in Canada. He is a *Chambers*-listed trial lawyer who acts for clients in complex business disputes, with significant experience in cross-border litigation and arbitration. John has been recognised by *Chambers*, *The Legal 500*, *Benchmark Litigation* and in *L'Expert*'s Annual Guide to the Leading Canada/US Cross-Border Litigation Lawyers. John's practice includes a significant fraud and financial crime component. He has appeared as counsel in a number of the country's leading corporate and civil fraud cases.

Baker & McKenzie LLP
181 Bay Street, Suite 2100
Toronto, Ontario, M5J 2T3
Canada

Tel: +1 416 865 2325
Fax: +1 416 863 6275
Email: john.pirie@bakermckenzie.com
URL: www.bakermckenzie.com

Baker McKenzie acts for many of the world's and Canada's largest multinationals, offering first-class domestic and cross-border legal advice on a range of business issues. With over 50 years of experience in the Canadian market, we are committed to helping clients fulfil their ambitions in an increasingly complex global marketplace.

Our Intellectual Property & Technology Practice Group is well known for developing and implementing strategies/programs to help clients efficiently navigate the Canadian and global regulatory landscape, as it pertains to issues that regularly arise across technology verticals. Our lawyers have expertise in a broad range of issues faced by industry participants, including intellectual property protection, data privacy, data security, cross-border data transfers, etc.

Our Litigation team has extensive experience in disputes focused on technology, media and telecommunications issues. Consistently top-ranked by leading market surveys, Baker McKenzie's commercial litigation practice represents clients in complex multi-jurisdictional litigation involving novel and precedent-setting issues.

www.bakermckenzie.com

China


Susan Ning


Han Wu

King & Wood Mallesons

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Under the Criminal Law of the People's Republic of China ("*Criminal Law*"), cybercrimes are mainly provided in the section: "Crimes of Disturbing Public Order". Articles 285, 286, and 287 are the three major Articles that directly relate to cybercrimes. Moreover, Article 253(1) indirectly relates to cybersecurity and applies to cases involving internet-related personal information infringement acts. The punishments for violating Articles 285, 286, and 287 include imprisonment, detention, and fines. For example, the offender may be sentenced to up to seven years' imprisonment for illegally obtaining data from a computer information system in serious cases. Entities may be convicted for violating Articles 285, 286, and 287, as unit crime has been provided for in all three Articles.

It is worth noting that Articles 286 and 287 set up the principle that if a person uses computers (for example, through hacking, phishing or other internet-related illegal action) to commit other crimes, i.e. crimes that traditionally had no relationship with the internet, such as financial fraud, theft, embezzlement, misappropriation of public funds and theft of state secrets, the offender shall be convicted of the crime for which the penalty is heavier.

Pursuant to Article 285 of the *Criminal Law*, activities that involve invading a computer information system in the areas of State affairs, national defence or advanced science and technology constitute the "crime of invading a computer information system". The offender shall be sentenced to a fixed-term imprisonment of not more than three years or detention. For activities of invading a computer information system other than those in the above areas, it may constitute a "crime of obtaining data from a computer information system and controlling a computer information system" and the offender shall be sentenced to a fixed-term imprisonment of not more than three years or detention, or imprisonment for three to seven years in serious cases. If an entity commits those crimes, such entities shall be fined, and the persons who are directly in charge and the other persons who are directly liable for the offences shall be punished accordingly.

Article 285 of the *Criminal Law* further provides that whoever, in violation of the state provisions, intrudes into a computer information system other than that prescribed in the preceding paragraph or uses other technical means to obtain the data stored, processed or transmitted in the said computer information system or exercise illegal control over the said computer information system shall, if the circumstances are serious, be sentenced to a fixed-term imprisonment of no more than three years or criminal detention, and/or be fined; or if the circumstances are extremely serious, shall be sentenced to a fixed-term imprisonment of no less than three years but not more than seven years, and be fined.

For example, in the criminal case of "*Zhang, Huang and others*' illegal obtainment of data in a computer information system and illegal control over a computer system", the defendant Zhang obtained the data by using hacker technology, and illegally obtained foreign citizens' credit card information, including the country, name, region, mailbox, phone number, credit card number, security code, validity period and other information from foreign shopping websites. Zhang then passed it on to Huang to sell online. According to the final decision of Jinhua Intermediate People's Court in Zhejiang Province in September 2020, the defendant Zhang was sentenced to five years' imprisonment and fined RMB 140,000 for illegally obtaining computer information system data. Defendant Huang was sentenced to four years and 11 months in prison and fined RMB 135,000 for illegally obtaining computer information system data.

It is noteworthy that the use of web crawlers may be regarded as invading conduct in violation of Article 285 if a technical method is adopted to crack anti-crawling measures set by websites or to bypass identity check processes set in a computer server. This is supported by various criminal cases in China. According to the ruling of the Yancheng Intermediate People's Court of Jiangsu Province on *Cheng Mao*'s case, the defendant Cheng Mao hired programmers to register batches of accounts of an online shopping website by using proxy pools or broadband dialling and changing IP addresses constantly to avoid the website's anti-crawling strategies and bypass the verification mechanism used in the account registration process. Then the defendant sold such accounts and obtained illegal gains of RMB 3,277,735. The court found that Cheng Mao was guilty of illegally obtaining data from a computer information system and sentenced them to four years in prison and a fine of RMB 500,000.

Pursuant to Article 29(1) of the Public Security Administration Punishments Law of the People's Republic of China ("*Public Security Administration Punishments Law*"), if a person, in violation of national regulations, invades a computer information system that causes harm to such system, he/she will be detained for not more than five days, and will be detained for more than five days but less than 10 days if the circumstances are serious.

Article 27 of the Cybersecurity Law of the People's Republic of China ("*Cybersecurity Law*") prohibits any person from

endangering network security, such as illegally intruding into any other person's network, interfering with the normal functions of any other person's network, and stealing network data. According to Article 63, any violation of the provision, if not regarded as committing a crime, will be subject to administrative penalties, including confiscation of illegal income, detention of no more than five days, and a fine between RMB 50,000 and RMB 500,000. If the circumstances are relatively serious, the violator shall be detained for not less than five days but not more than 15 days, and may be fined between RMB 100,000 and RMB 1,000,000. Where an entity carries out any of the above conduct, the public security authority shall confiscate its illegal income, impose a fine of between RMB 100,000 and RMB 1,000,000, and punish its directly responsible person in charge and other directly liable persons in accordance with the provisions of the preceding paragraph. Article 63 of the *Cybersecurity Law* further provides that the person given a public security punishment due to his/her violation of Article 27 shall not hold a key position of cybersecurity management and network operation for five years; and a person given any criminal punishment shall be prohibited for life from holding a key position of cybersecurity management and network operation.

Denial-of-service attacks

Pursuant to Article 286 of the *Criminal Law*, denial-of-service attacks could constitute the "crime of sabotaging [a] computer information system", and a sentence of more than five years' imprisonment may be given in particularly serious cases.

Denial-of-service attacks may also lead to administrative penalties. Pursuant to Article 29(2) of the *Public Security Administration Punishments Law*, if a person, in violation of national regulations, deletes, changes, increases or interferes with the functions of a computer information system, making it impossible for the system to operate normally, an administrative penalty of detention of less than five days, or in serious cases, detention of more than five days but less than 10 days, will be imposed.

In terms of *Cybersecurity Law*, a denial-of-service attack will also be regarded as endangering network security and will also be subject to penalties under Article 63 of the *Cybersecurity Law*.

Phishing

Phishing is usually performed to steal or otherwise acquire the personal information of citizens, which is considered the "crime of infringing a citizen's personal information" provided in Article 253(1); up to seven years' imprisonment may be sentenced in serious cases. In addition, those who engage in fraudulent activities by way of phishing may also commit the crime of "fraud". If the amount involved is relatively large, the offender will be sentenced to three years or fewer in prison or put under limited incarceration or surveillance, in addition to being fined. Those who defraud extraordinarily large amounts of money and property, or who are involved in especially serious cases, are to be sentenced to 10 years or more in prison or even be given life sentences, in addition to fines or confiscation of property.

According to the judgment made by the Nanping Intermediate People's Court of Fujian Province in April 2021, the defendants Xie and Lin sent phishing QR codes to the victims after adding their WeChat accounts. After the victims have scanned the QR codes, and filled in their personal bank account numbers, passwords and other information, the defendants checked the personal bank information of the victims and inquired about the balance in their accounts. Then, based on the search results, the defendants used different methods to defraud. Finally, Xie, Lin, and other plaintiffs were convicted of fraud. Xie was sentenced to eight years in prison and a fine of RMB 80,000, while Lin was sentenced to seven years in prison and a fine of RMB 70,000.

Furthermore, as most phishing is conducted by spreading a computer virus, the administrative penalty for this is for detention of less than five days or, in serious cases, detention of more than five days but less than 10 days, pursuant to Article 29 of the *Public Security Administration Punishments Law*. Article 63 of the *Cybersecurity Law* may also apply.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

For intentional creation or dissemination of a computer virus or other destructive programs, including, but not limited to, ransomware, spyware, worms, trojans and viruses, which affect the normal operation of a computer information system, if serious consequences are caused, such activities constitute the "crime of sabotaging a computer information system" under Article 286 of the *Criminal Law*. The offender may be sentenced to five years' imprisonment in serious cases.

In addition, anyone who installs the above destructive programs in order to control others' computers may commit the crime of illegally controlling the computer information system under Paragraph 2 of Article 285 of the *Criminal Law*. If the circumstances are serious, he/she will be sentenced to imprisonment of not more than three years or limited incarceration, and/or be fined; or, if the circumstances are extremely serious, he/she shall be sentenced to imprisonment of not less than three years but not more than seven years, and be fined.

For instance, in the case of Ling illegally controlling the computer information system, the defendant, without permission of the owner of the Internet bar, installed the destructive Trojan horse program on the Internet bar server, and illegally controlled the computer information system. According to the final judgment made by the Dongguan Intermediate People's Court in April 2021, the defendant Ling was sentenced to three years in prison, and fined RMB 5,000 for the crime of illegal control of the computer information system.

In addition, intentionally making up or transmitting such destructive programs that adversely affect the normal operation of a computer information system is illegal, pursuant to Article 29 of the *Public Security Administration Punishments Law*. The violator may be subject to detention of less than five days or, in serious cases, detention of more than five days but less than 10 days. Article 63 of the *Cybersecurity Law* may also apply.

Moreover, Article 47 of the *Cybersecurity Law* provides that electronic information sent by and application software provided by any individual or organisation shall not be installed with malware, and the violator, according to Article 60 of the *Cybersecurity Law*, will be ordered to take corrective action and be given a warning by the competent authorities. If the violator refuses to take corrective action, or such consequences as endangering cybersecurity are caused, it shall be fined between RMB 50,000 and RMB 500,000, and the directly responsible person in charge shall be fined between RMB 10,000 and RMB 100,000.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

If a person provides hardware, software or other tools specially used for invading or illegally controlling computer information systems, or if the person knows that any other person is committing the criminal act of invading or illegally controlling a computer information system and still provides programs or tools for such a person, he/she shall commit the crime of "providing program[s] or tools for invading or illegally controlling computer information systems", pursuant to Article 285 of the *Criminal Law*.

In addition, if a person intentionally makes up or transmits destructive programs such as computer viruses that adversely

affect the normal operation of a computer information system, and if not severe enough to constitute a crime, he/she will be penalised according to Article 29 of the *Public Security Administration Punishments Law*. Furthermore, Articles 27 and 63 of the *Cybersecurity Law* also prohibit provision of programs or tools specifically used for conducting any activity endangering cybersecurity, or provision of technical support, advertising promotions, payments and settlement services or any other assistance to any person conducting any activity endangering cybersecurity.

Possession or use of hardware, software or other tools used to commit cybercrime

If a person possesses or uses hardware, software or other tools to commit cybercrime as prescribed under the *Criminal Law*, depending on the crime committed, the offender may be convicted in accordance with the corresponding Article under the *Criminal Law*, such as the "crime of invading a computer information system".

There is also an offence, i.e. "illegal use of information networks", that involves activities that take advantage of an information network to establish websites and communication groups for criminal activities, such as defrauding, teaching criminal methods, producing or selling prohibited items and controlled substances. If the criminal activity also constitutes another offence, the offender shall be convicted of the crime that imposes a heavier penalty.

Identity theft or identity fraud (e.g. in connection with access devices)

Under the *Criminal Law*, for identity theft, if the offender obtains identities by stealing or otherwise illegally acquires the personal information of citizens, such activity may be convicted as the "crime of infringing a citizen's personal information", pursuant to Article 253(1). If a person uses the stolen identity of others as his/her own proof of identity, such behaviour may constitute the "crime of identity theft" under Article 280(1) of the *Criminal Law*; in case such person uses the stolen identity to commit fraud or other criminal activities, he/she should be convicted of the crime the penalty of which is higher.

The *Cybersecurity Law* protects network information security, including the security of personal information. Stealing or illegally acquiring the personal information of citizens may also cause administrative penalties if the violation is not severe enough to constitute a crime.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

If a current or former employee breaches confidentiality obligations and causes infringement of personal information, trade secrets, or state secrets, etc., the offender will be convicted pursuant to Article 287 and punished in accordance with the relevant provisions of the *Criminal Law*, such as the "crime of infringing trade secrets".

In the final judgment made by the Huizhou Intermediate People's Court in September 2020, the defendant Wang left Huaxing Company and started working for Chongqing Huike Company. Huike Company wanted to inquire about the reasons for the abnormal product experiment. After Wang knew this, he shared the undisclosed production process and technology reports, which he obtained from Huixing Company in the WeChat group of the department of Huike Company, resulting in the use of such technical information by Huike Company. The court finally ruled that the defendant Wang constituted the crime of infringing trade secrets.

Furthermore, the infringement of trade secrets, under the Anti-unfair Competition Law of the People's Republic of China (the "*Anti-unfair Competition Law*"), will be subject to administrative penalties, including being ordered to cease the infringing conduct, the confiscation of illegal income, a fine ranging from RMB 100,000 to RMB 1 million, and a fine ranging from RMB 500,000 to RMB 5 million if the circumstances are serious.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Unsolicited penetration testing could be seen as an illegal invasion of another person's computer information system, without having prior permission or consent.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

If a person, in violation of laws and regulations, deletes, amends, adds or disturbs the functions of a computer information system and causes the computer information system's inability to work normally, or conducts operations of deletion, amendment or addition towards the data or application programs that are stored, disposed of or transmitted in a computer information system, and serious consequences result, such activities constitute the "crime of sabotaging [a] computer information system" under Article 286 of the *Criminal Law*. The offender shall be sentenced to a fixed-term imprisonment of more than five years if serious consequences result.

If a person, in violation of national regulations, deletes, changes, or increases the stored, processed, or transmitted data and the application program of a computer information system, the person shall be detained for less than five days, or in serious cases, detained for more than five days but less than 10 days, pursuant to Article 29 of the *Public Security Administration Punishments Law*. Furthermore, any conduct, in addition to what is described above, that endangers network security will be regulated under Articles 27 and 63 of the *Cybersecurity Law*.

1.2 Do any of the above-mentioned offences have extraterritorial application?

All of the above-mentioned crimes have extraterritorial application. Firstly, if the criminal act or its consequences take place within the territory of China, the crime shall be deemed to have been committed within the territory of China. Secondly, the *Criminal Law* is applicable to citizens of China who commit crimes prescribed in the *Criminal Law* outside the territory of China; however, if the maximum penalty of such crime prescribed in the *Criminal Law* is a fixed-term imprisonment of not more than three years, the offender could be exempted from punishment. Thirdly, if a foreigner commits a crime outside the territory of China against the State or against Chinese citizens, the offender may be convicted pursuant to the *Criminal Law* if the *Criminal Law* prescribes a minimum punishment of fixed-term imprisonment of not less than three years; however, the *Criminal Law* shall not apply if it is not punishable according to the law of the place where it was committed.

The *Public Security Administration Punishments Law* is applicable within the territory of China (except where specially provided for by other laws), or to acts against the administration of public security committed aboard ships or aircrafts of China (except where specially provided for by other laws).

The *Cybersecurity Law* generally applies to the construction, operation, maintenance and use of the network within the territory of China. Where any overseas institution, organisation or

individual attacks, intrudes into, disturbs, destroys or otherwise damages the critical information infrastructure ("*CII*") of China, causing any serious consequence, the violator shall be subject to legal liability; and the public security department of the State Council and relevant authorities may decide to freeze the property of or take any other necessary sanctions measure against the institution, organisation or individual.

The *Anti-unfair Competition Law* does not explicitly provide that it has extra-terrestrial application. In principle, any conduct that disrupts market competition or harms the legitimate rights and interests of business operators or consumers will be regulated under this law.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

For the above-mentioned offences, there are no specific mitigation conditions prescribed by law. However, the mitigation conditions prescribed in the *Criminal Law* for all crimes are applicable. For example, if an offender voluntarily gives oneself up to the police and confesses his/her crimes or exposes others' crimes that can be verified, the offender would be given a mitigated punishment.

The *Anti-unfair Competition Law* provides in Article 25 that where a business operator who engages in unfair competition takes the initiative to eliminate or mitigate the harmful consequences of the illegal act, the administrative punishment shall be reduced or mitigated; where the illegal act is trivial and promptly corrected and does not cause harmful consequences, no administrative punishment shall be imposed. The Law of the People's Republic of China on Administrative Penalty (the "*Administrative Penalty Law*") generally sets out circumstances where the administrative penalties could be mitigated, including taking the initiative to eliminate or mitigate the harmful consequences of the illegal act, being coerced by another person to commit the illegal act, and performing meritorious deeds in coordination with the authorities to conduct an investigation, etc.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The *Cybersecurity Law*, which came into force on 1 June 2017, is the law covering various aspects of network security and has laid the foundation for a comprehensive cybersecurity regulatory regime in China. So far, a series of specific measures aimed at facilitating the implementation of the *Cybersecurity Law* have already been enacted, such as the *Measures for Cybersecurity Review*, the *National Emergency Response Plan for Cybersecurity Incidents*, and the *Provisions on Protection of Children's Personal Information Online*.

The *Cybersecurity Law* recognises the graded cybersecurity protection as the basic legal system to ensure network security in China. While the *Regulation on Graded Protection of Cybersecurity* is still seeking opinions, relevant authorities have officially been promulgating recommended national standards regarding graded cybersecurity protection since May 2019 for guiding the graded protection. These national standards include, but are not limited to: the *Information Security Technology-Baseline for Classified Protection of Cybersecurity* (GB/T 22239-2019), which replaces GB/T 22239-2008; the *Information Security Technology-Evaluation Requirement for Classified Protection of Cybersecurity* (GB/T 28448-2019), which replaces GB/T 28448-2012; the *Information Security Technology-Technical Requirement of Security Design for Classified Protection of Cybersecurity* (GB/T 25070-2019), which replaces GB/T 25070-2010; the *Implementation Guide for Classified Protection Of Cybersecurity* (GB/T 25058-2019), which replaces GB/T 25058-2010; and the *Classification Guide for Classified Protection Of Cybersecurity* (GB/T 22240-2020), which replaces GB/T 22240-2008.

Meanwhile, the regulations and guidelines on the protection of CII, data processing and security assessment of outbound data transfers have been released, including the *Regulations on the Security Protection of Critical Information Infrastructure*, which was promulgated in July 2021 and took effect on 1 September 2021, the *Measures for Cybersecurity Censorship (Draft for Comments)*, which was issued for public comments in July 2021, and the *Administrative Provisions on Security Loopholes of Network Products (Draft for Comments)*.

It is worth noting that in June 2021, China promulgated the Data Security Law of the People's Republic of China ("*Data Security Law*"), which governs the collection, storage, processing, use, supply, transaction and disclosure of various types of data. The *Data Security Law* has established a data classification and grading system, and relevant authorities will also formulate catalogues of "important data" within their jurisdictions, and implement enhanced security measures to protect such important data. It also stipulates that data activities that may affect national security will be subject to security reviews organised by relevant authorities. As a specific industry regulation under the *Data Security Law*, five government agencies, including but not limited to the Cyberspace Administration of China ("*CAC*"), and the National Development and Reform Commission, issued the *Administrative Provisions on the Security of Automobile Data (for Trial Implementation)* on 16 August 2021, which: define the basic concepts related to automobile data processing; and clarify the legal obligations of automobile data processors as well as the processing standards for important data and sensitive personal information. Moreover, the local regulation *Regulations of Shenzhen Special Economic Zone on Data*, previously released by the Shenzhen Municipal People's Congress, also set out rules of data processing and sharing, opening, utilisation of public data.

Furthermore, China has strengthened the regulations of personal information collection. On 20 August 2021, the Personal Information Protection Law of the People's Republic of China ("*Personal Information Protection Law*") was released, which contained comprehensive rules on various matters to which attention should be paid in personal information processing. Regarding the regulation on the processing of personal information by app operators, several regulative documents or guidelines, including the *Guide to the Self-Assessment of Illegal Collection and Use of Personal Information by Apps*, the *Methods for Determining the Illegal Collection and Use of Personal Information by Apps*, and the *Guide to Self-Assessment of the Collection and Use of Personal Information by Apps*, etc., have been issued.

Moreover, the Cryptography Law of the People's Republic of China ("*Cryptography Law*"), which came into effect on 1 January 2020, provides regulations on the management and use of cryptography.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The *Cybersecurity Law* includes provisions on the security protection

of CII. In addition, the *Regulations on the Security Protection of Critical Information Infrastructure* further set out requirements on the security protection of CII. For example, operators of CII shall set up special security management departments, prepare contingency plans, and conduct regular contingency drills, network security inspections and risk assessments, etc.

Also, Article 27 of the *Cryptography Law* provides that for CII operators, laws, administrative regulations, and relevant national regulations require protection by commercial cryptography; thus, the CII operators thereof shall use commercial cryptography for protection and conduct a security assessment of commercial cryptography applications.

The *Measures for Cybersecurity Censorship (Draft for Comments)* issued in July 2021, requires that CII operators purchasing network products and services while data processors carry out data processing that affects or may affect national security, shall conduct cybersecurity reviews in accordance with the Measures.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes. The *Cybersecurity Law*, the *Data Security Law*, the *Personal Information Protection Law*, the *Administrative Provisions on the Security of Automobile Data (for Trial Implementation)*, the *Regulations on the Security Protection of Computer Information System*, the *National Emergency Response Plan for Cybersecurity Incidents*, and other relevant laws and regulations have provided for network operators' legal duties when facing cybersecurity Incidents, which in general could be categorised into the following:

(1) **regular preventive work**: network operators must adopt regular measures to prevent cybersecurity Incidents, including adopting technical measures to prevent cybersecurity violations such as computer viruses, cyberattacks and network intrusions, monitoring and recording the network operation status and cybersecurity events, and maintaining cyber-related logs for no less than six months. Furthermore, network operators shall provide early warnings of abnormalities such as data leakage, damage, loss and tampering, etc. Important data processors and sensitive personal data processors shall also carry out regular risk assessments.
Moreover, under Article 58 of the *Personal Information Protection Law*, personal information processors that provide important Internet platform services involving a huge number of users and complicated business types shall perform the following obligations: (a) establishing and improving the system of personal information protection compliance rules in accordance with the provisions issued by the state, forming independent institutions mainly consisting of external personnel to supervise personal information protection; (b) following the principles of openness, fairness and impartiality, developing platform rules, and clarifying the norms for the processing of personal information by product or service providers on platforms and the obligations to protect personal information; (c) stopping providing services to product or service providers on platforms that process personal information in severe violation of laws and administrative regulations; and (d) issuing social responsibility reports on personal information protection on a regular basis to be subject to public supervision;

(2) **emergency measures for security Incidents**: network operators must develop an emergency plan for cybersecurity Incidents in order to promptly respond to security risks, to take remedial actions immediately, to notify affected data subjects, and to report the case to the competent authorities as required. In addition, the *Regulations of Shenzhen Special Economic Zone on Data* stipulate in detail that data security contingency plans should classify data security Incidents based on factors such as the degree of harm and the scope of impact, and provide corresponding contingency measures; and

(3) **after-action review**: to keep communication with and assist the authorities in finishing their investigation and review after an Incident, such as providing a summary of the cause, nature, and influence of the security Incident and improvement measures.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes, they are.

(1) The reporting obligation will be triggered by the occurrence of an Incident threatening network security.

(2) Pursuant to the *Cybersecurity Law,* the *Data Security Law* and relevant regulations, network operators shall at least timely notify the local government, industry regulators, public security authorities and local cyberspace administrations. Where a data security Incident occurs during data processing, measures shall be taken forthwith and reports shall be made to the relevant departments as required. Also, pursuant to the *Regulations of the People's Republic of China on the Security Protection of Computer Information System*, any case arising from computer information systems shall be reported to the public security authority within 24 hours. Moreover, if there is a possibility of information leakage related to national security, the national security authorities shall also be informed.

(3) At least the following contents are required to be reported: information of the notification party; description of the network security Incident; detailed information about the Incident; nature of the Incident; affected properties (if any); personal information being affected/breached (if any); preliminary containment measures that have been taken; and preliminary assessment on the severity of the Incident.

(4) If the publication of Incident-related information will jeopardise national security or public interest, then such publication shall be prohibited.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes, they are.

Under the *Cybersecurity Law*, in case of disclosure, damage or loss, or possible disclosure, damage or loss, of user information, the network operator is obligated to take immediate remedies and notify the affected users promptly. In addition, for any risk, such as a security defect or bug that is found in a network product or service, the product/service provider concerned shall inform the users of the said risk.

Furthermore, pursuant to the *Data Security Law*, in data-processing activities, one shall make contingency plans, take disposition measures immediately, and notify users and report to the appropriate department in a timely manner as required, when a data security event occurs.

Currently, relevant laws and regulations do not provide specific requirements regarding the nature and scope of information to be reported; according to the *Information Security Techniques – Personal Information Security Specification*, recommended standards formulated by the National Standardization Committee, operators shall at least inform data subjects of the general description of the Incident and its impact, any remedial measures taken or to be taken, suggestions for individual data subjects to mitigate risks, and contact information of the person responsible for dealing with the Incident, etc.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

Any regulators identified under question 2.4 above to which network operators are required to report an Incident shall have the authority to enforce the requirements identified under questions 2.3 to 2.5. Specifically, the enforcement authorities include the CAC, the Ministry of Industry and Information Technology ("*MIIT*"), the Ministry of Public Security ("*MPS*"), the State Secrecy Bureau, the State Encryption Administration and industry regulators, etc.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Pursuant to the *Cybersecurity Law*, in case of non-compliance, network operators may be given a warning, ordered to take rectification measures, and/or imposed fines by the relevant authorities. In case of refusal to make rectifications or in severe circumstances, further penalties such as suspension of related business, winding up for rectification, shutdown of websites, and revocation of a business licence may be imposed by the competent authorities.

Furthermore, under the *Personal Information Protection Law*, where a personal information processor processes personal information in violation of this law or fails to fulfil the personal information protection obligations as provided in this Law, the department performing personal information protection functions shall also confiscate its or his/her illegal income. Moreover, where any violation of laws as prescribed in this Law is committed, it shall be entered into the relevant credit record and be published in accordance with the provisions of the relevant laws and administrative regulations.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

On 2 July 2021, the Cybersecurity Review Office under the CAC initiated a cybersecurity review of an online car-hailing app and certain other online apps in accordance with the *Measures for Cybersecurity Review*. To cooperate with the cybersecurity review and to prevent the expansion of risks, the app operators were ordered to suspend the registration of new users during the period of review. Currently, the cybersecurity review is still ongoing.

Moreover, each year, the CAC, MIIT, and MPS, together with the National Work Group for "Combating Pornography and Illegal Publications", initiate a special campaign called "Jingwang" (clean the internet), aiming at investigating and preventing illegal activities in cyberspace or cybercrimes.

This year, the "Jingwang" action focuses on screening online live streaming, social contact, forums and communities, online comics and other fields, and achieved phased results. By the end of May 2021, regulatory authorities had disposed of more than 1.55 million pieces of harmful online information, banned and closed over 6,400 illegal websites, and investigated and handled 960 cases of cracking down on online pornography and illegal publications.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
The use of Beacons may result in the collection and use of users' personal information. Pursuant to the *Cybersecurity Law*, organisations shall notify users and obtain their consent before collecting information. Considering the difficulty of obtaining consent when collecting information through Beacons, they are generally regarded as not complying with the basic requirements under the *Cybersecurity Law*.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Relevant laws and regulations do not explicitly prohibit organisations from using Honeypots to detect and deflect Incidents in their own network.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Relevant laws and regulations do not explicitly prohibit organisations from using Sinkholes to detect and deflect Incidents in their own network.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Monitoring or intercepting electronic communications may trigger privacy issues, as they usually involve collection of private or personal communication information. The Civil Code of People's Republic of China ("*Civil Code*"), which will be enacted on 1 January 2021, explicitly prohibits individuals or organisations from infringing upon a natural person's right to privacy. Specifically, Article 1033 of the *Civil Code* provides that unless otherwise prescribed by the law or specifically agreed by the right holders, no organisation or individuals are allowed to deal with the private information of others.

Furthermore, Article 65 of the Telecommunications Regulations of the People's Republic of China ("*Telecommunications Regulations*") provides that except for the inspection of telecommunications contents by the public security authorities, the national security authorities, or the People's Procuratorate in accordance with the procedures stipulated by the law for the purposes of national security or a criminal investigation, no organisation or individual shall inspect telecommunications contents for any reason.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Pursuant to Article 28 of the *Cryptography Law*, the commerce department of the State Council and the state cryptography administration shall implement import licensing for commercial cryptography that involves State security and public interest and that have encryption protection functions. They shall implement export controls on commercial cryptography that involves State security and public interest or that involves the international obligations of China.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Although industries or sectors such as telecoms, credit reporting, banking and finance, and insurance have some specific requirements with respect to the collection and protection of information, the prevention of information leakage, and the emergency response to Incidents, these requirements are, in general, in line with those under the *Cybersecurity Law*, the *Data Security Law*, and the *Personal Information Protection Law* without deviations.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Yes. For example, the *Provisional Rules on Management of the Individual Credit Information Database* are promulgated by the People's Bank of China to ensure the secure and legitimate use of personal credit information, the *Measures of the People's Bank of China for the Protection of Financial Consumers' Rights and Interests* (updated by the People's Bank of China in September 2020) obliges financial institutions to ensure the security of personal financial information, and the *Anti-Money Laundering Law*, as well as the *Administrative Measures for the Identification of Clients and the Keeping of Clients' Identity Information and Transaction Records by Financial Institutions*, require financial institutions to take technical measures to prevent the loss, destruction or leakage of their client's identity information or transaction data. In addition, pursuant to the *Provisions on Protecting the Personal Information of Telecommunications and Internet Users*, telecommunication business operators or internet information service providers shall record information such as the staff members who perform operations on the personal information of users, the time and place of such operations, and the matters involved, to prevent user information from being divulged, damaged, tampered with or lost.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Under the *Cybersecurity Law*, if a company, as a network operator, fails to fulfil the obligation of security protection to ensure that the network is free from interference, disruption or unauthorised access, and to prevent network data from being disclosed, stolen or tampered with, fails to satisfy the mandatory requirements set forth in the applicable national standards, or fails to develop an emergency plan for cybersecurity Incidents, a warning shall be imposed on the company, and a fine will be imposed on both the company and the responsible person directly in charge if such company refuses to make rectifications or causes threats to cybersecurity.

Furthermore, under the *Data Security Law*, where an organisation conducting data processing activities fails to conduct regular risk assessments, strengthen risk monitoring or take remedial measures after any data security defect, vulnerability, or other risk is discovered, the competent authority may impose a fine on the directly liable executive in charge or other directly liable person.

Moreover, where a personal information processor commits any illegal act as specified in the preceding paragraph with serious circumstances, the authority performing personal information protection functions at or above the provincial level shall: order it or him/her to take corrective action; confiscate its or his/her illegal income; and impose a fine, and may also: order the suspension of relevant business or suspension of business for an overhaul; notify the relevant competent department to revoke the relevant business permit or business licence; and impose a fine on any directly liable person in charge or other directly liable person, and may decide to prohibit them from serving as directors, supervisors, senior executives or persons in charge of the personal information protection of related enterprises during a certain period of time.

In addition, as mentioned in question 1.1 above, pursuant to Article 286(1) of the *Criminal Law*, if a network service provider fails to perform its duties of security protection on the information network as required by laws and administrative regulations, and refuses to correct their conduct after the regulatory authorities order them to rectify the non-performance, the network operator shall be fined, and the persons directly in charge and the other persons directly liable for the offences may be sentenced.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Under the *Cybersecurity Law*, all network operators are required to designate a person in charge of cybersecurity, such as a chief information security officer ("*CISO*"), to establish an emergency plan for cybersecurity Incidents, and to take technical measures to monitor and record network operation and cybersecurity events. In addition, pursuant to Article 38 of the *Cybersecurity Law*, CII operators are required to conduct, by themselves or entrusting a service provider, an examination and assessment of their cybersecurity and the potential risks at least once a year, and submit the examination and assessment results, as well as improvement measures, to the competent authorities in charge

of the security of the CII. That is to say, periodic cyber risk assessments and vulnerability assessments are mandatory for CII operators. Furthermore, critical network equipment and special-purpose cybersecurity products provided by third-party vendors should satisfy the compulsory requirements set forth in the national standards and shall not be sold or supplied until such equipment or product successfully passes security certification or security tests by a qualified organisation.

Under the *Data Security Law*, a processor of important data shall specify the person(s) responsible for data security and the management body, and implement the responsibility of data security protection. Moreover, under Article 30 of the *Data Security Law*, the processor of important data shall carry out regular risk assessment on their data processing activities and submit a risk assessment report to the relevant competent authority.

The *Personal Information Protection Law* also requires that a personal information processor that processes the personal information reaching the threshold specified by the national cyberspace administration in terms of quantity shall appoint a person in charge of personal information protection to be responsible for overseeing personal information processing activities as well as the protection measures taken, among others. Article 51 requires that all personal information processors shall take necessary measures, including but not limited to: developing and organising the implementation of emergency plans for personal information security Incidents; and conducting classified management of personal information to ensure that personal information processing activities comply with the provisions of laws and administrative regulations, and prevent unauthorised access as well as the leakage, tampering or loss of personal information. The Article 55 further stipulates that a personal information processor shall conduct an impact assessment on personal information protection beforehand in the following circumstances: (i) processing sensitive personal information; (ii) making use of personal information to make automatic decision-making; (iii) entrusting others to process personal information, providing other personal information processors with personal information, and publicising personal information; (iv) providing personal information to overseas parties; or (v) other personal information processing activities that have a significant impact on personal rights and interests.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Please refer to the answers to questions 2.4 and 2.5 above.

In addition, listed companies may have the duty to disclose cybersecurity risks or Incidents to the China Securities Regulatory Commission or disclose such information in their annual reports, depending on whether such information is deemed as significant and required to be disclosed.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

From the perspective of individuals, if an Incident results in unauthorised access to or disclosure of personal information collected and kept by the network operator, the individuals affected could bring a lawsuit against such network operator for breach of security protection obligations or for disclosing personal information by negligence on the basis of tort pursuant to the *Civil Code* and the *Personal Information Protection Law*. In two private lawsuits brought by consumers in July 2020, the court of first instance gave its verdict that the defendants in both cases had infringed consumers' rights and interests regarding personal information.

Further, as confirmed by the decision in the *Sina/Maimai* case ruled by the Beijing Intellectual Property Court, user data/information is an important operating resource and confers competitive advantages to network operators. If a network operator "steals" data from its competitor by accessing the data of such competitor without authorisation, the aggrieved party could sue the infringing party for unfair competition on the basis of the *Anti-unfair Competition Law*.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

On 9 August 2017, the plaintiff Shen ordered two airline tickets through an online booking app Ctrip App. Shen then received a text message that his flight was cancelled due to mechanical failure and he would be given a refund and compensation. Shen called the "customer service phone number", and the "customer service" accurately identified the name of the passenger, flight departure time and flight number. After Shen transferred RMB 99,976 to the "customer service", he finally realised that he had been deceived.

On 29 December 2018, the Chaoyang District People's Court of Beijing announced the following judgment: Ctrip had breached its security obligation as a network operator, resulting in security maintenance loopholes in the protection of the user's personal information. Therefore, Ctrip shall compensate Shen RMB 50,000 for his economic loss and make an apology to him at the same time.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Please refer to the answer to question 6.1.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations may take out insurance against Incidents, provided that such insurance categories are within the permitted scope of insurance regulations and have been approved by or filed with the China Insurance Regulatory Commission ("*CIRC*"). Currently, in China, there are already several insurance agents providing insurance related to Incidents such as data leakage, hacking, etc.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

So far, we are not aware of any regulation that sets out limitations specifically on insurance against Incidents. Normally,

the coverage of loss will be decided through private negotiation between the insurer and the applicant, as long as such coverage does not violate mandatory regulations in China.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

In accordance with the *Cybersecurity Law* and other relevant regulations, generally there are several enforcement agencies that are entitled to have investigatory power regarding an Incident, such as:

(1) the CAC, which is responsible for the overall planning and coordination of cybersecurity work and the relevant supervision and administration; and

(2) the authority in charge of telecommunication, the public security authority and other relevant authorities of the State Council, which will take charge of protecting, supervising and administrating cybersecurity pursuant to the present regulations in China.

The specific investigatory power of the above enforcement agencies can be found in a number of laws and regulations. For example, as stated in Article 54 of the *Cybersecurity Law*, the relevant departments of the government at provincial level and above are entitled to take the following measures in case of an increasing risk of an Incident:

(1) require authorities, organs and personnel concerned to promptly collect and report necessary information;

(2) organise authorities, organs and professionals concerned to analyse and evaluate cybersecurity risks; and

(3) give warnings to the public about the cybersecurity risks and release prevention and mitigation measures.

Pursuant to Article 19 of the Anti-Terrorism Law of the People's Republic of China ("*Anti-Terrorism Law*"), where a risk of terrorism may arise in an Incident, the CAC, competent telecommunications department, public security department, as well as the national security department shall carry out the following actions in accordance with their respective duties:

(1) order the relevant entities to stop transmission and delete the information involving terrorism and extremism; and

(2) shut down the relevant sites and cease the related services.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

First, the *Cybersecurity Law* has made it clear that network operators shall provide technical support for the public security department and the national security department specifically on two matters: (1) safeguarding national security; and (2) investigation of crimes. Second, the *Anti-Terrorism Law* explicitly states that telecommunications operators and internet service providers shall facilitate the relevant departments in terrorism cases, such as providing technical interfaces and decryption services. Moreover, for entities and individuals that engage in international network connections, public security departments may also ask them to provide information, materials and digital files on security protection matters when investigating crimes committed through computer networks connected with international networks. In several business sectors, such as the financial sector, there are also applicable laws or regulations requiring entities to coordinate with relevant industrial regulators in their investigatory activities. For example, the *Anti-Money Laundering Law* requires financial institutions to promptly report transactions of large amounts and suspicious transactions to the anti-money laundering information centre.

Susan Ning is a senior partner and the head of the Commercial and Regulatory Group. She is one of the pioneers engaged in the cybersecurity and data compliance practice, with publications in a number of journals such as the *Journal of Cyber Affairs*. Her articles include "New Trends of the US Personal Data Protection – Key Points of the New FCC Rules", "Big Data: Success Comes Down to Solid Compliance", "Does Your Data Need a "VISA" to Travel Abroad?", and "A Brief Analysis on the Impact of Data on Competition in the Big Data Era", among others. Susan is recognised as a "Tier 1 Lawyer" for Cybersecurity and Data Compliance in 2019 *LEGALBAND* China.
Susan's practice areas cover self-assessment of network security, responding to network security checks initiated by authorities, data compliance training, due diligence of data transactions or exchanges, compliance of cross-border data transmissions, etc. Susan has assisted companies in sectors such as IT, transportation, online payments, consumer goods, finance, and the Internet of Vehicles in dealing with network security and data compliance issues.

King & Wood Mallesons
18th Floor, East Tower, World Financial Center
No.1 Dongsanhuan Zhonglu, Chaoyang District
Beijing 100020
China

Tel: +86 10 5878 5010
Email: susan.ning@cn.kwm.com
URL: www.kwm.com

Han Wu practises in the areas of cybersecurity, data compliance and antitrust. He excels in providing cybersecurity and data compliance advice to multinational companies' branches in China from the perspective of data compliance in China. Han also has expertise in establishing network security and data compliance systems for Chinese enterprises going abroad in line with the requirements of the European Union (GDPR), the United States and other jurisdictions. Han was elected as one of "40-under-40 Data Lawyers" by *Global Data Review* in 2018. Han was also recognised as a "Next Generation Partner" by *The Legal 500* in 2021 and named one of the 2021 *ALB* China Top 15 TMT Lawyers.
In the areas of cybersecurity and data compliance, Han provides legal services including: assisting clients to establish a cybersecurity compliance system; assisting clients in self-investigation on cybersecurity and data protection; assisting clients to conduct internal training on cybersecurity and data compliance; assisting clients in due diligence in data transactions; assisting clients to design plans for cross-border data transfers; and assisting clients in network security investigations and cybersecurity Incidents, among others.

King & Wood Mallesons
18th Floor, East Tower, World Financial Center
No.1 Dongsanhuan Zhonglu, Chaoyang District
Beijing 100020
China

Tel: +86 10 5878 5749
Email: wuhan@cn.kwm.com
URL: www.kwm.com

King & Wood Mallesons is an international law firm headquartered in Asia that advises Chinese and overseas clients on a full range of domestic and cross-border transactions, providing comprehensive legal services. Around the world, the firm has over 2,000 lawyers with an extensive global network of 27 international offices spanning Singapore, Japan, the US, Australia, the UK, Germany, Spain, Italy and other key cities in Europe as well as presences in the Middle East. With a large legal talent pool equipped with local in-depth and legal practice, it provides legal services in multiple languages. King & Wood Mallesons, with its strong foundation and ever-progressive practice capacity, has been a leader in the industry. It has received more than 300 international and regional awards from internationally authoritative legal rating agencies, businesses and legal media, including Acritas, *The Financial Times*, *ALB*, *Who's Who Legal*, *Chambers Asia-Pacific* Awards, *Euromoney*, *LEGALBAND*, *Legal Business*, *The Lawyer*, etc.

www.kwm.com

KING&WOOD MALLESONS
金杜律师事务所

England & Wales


Nigel Parker


Benjamin Scrace

Allen & Overy LLP

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Yes. Under the Computer Misuse Act 1990, it is an offence to cause a computer to perform any function with the intent to secure unauthorised access to any program or data held in a computer (or enable such access to be secured). On indictment, the maximum penalty is two years' imprisonment. If a person commits this offence with the intent to commit or facilitate a more serious "further offence" (e.g. theft via the diversion of funds), the maximum penalty is five years' imprisonment. In 2019, a director of a CCTV provider and her employee were sentenced to 14 months' and five months' imprisonment (respectively) after they accessed CCTV footage of the post-mortem of footballer Emiliano Sala. In 2019, a disgruntled former IT contractor at Jet2 was sentenced to 10 months' imprisonment after he deleted user accounts and accessed the email account of the Jet2 CEO in a revenge attack.

The offence can also arise alongside the criminal offences in the Data Protection Act 2018, to the extent the offence involves causing a computer to perform a function with the intention of securing unauthorised access to data. For example, in a prosecution brought by the Information Commissioner's Office (ICO) in January 2021 under the Data Protection Act 2018 and the Computer Misuse Act 1990, an employee for RAC was sentenced to eight months' imprisonment and subject to a £25,000 confiscation order following the unauthorised access and transfer of customer personal data to a third-party accident claims management firm.

Under the Investigatory Powers Act 2016 (**IPA 2016**), it is an offence to intercept intentionally (within the UK) a communication in the course of its transmission by means of a public or private telecommunications system without lawful authority. The offence is punishable on a summary conviction (with a fine) and on conviction on indictment (with up to two years' imprisonment or a fine, or both).

Denial-of-service attacks
Yes. Under the Computer Misuse Act 1990, it is an offence to do any unauthorised act in relation to a computer that a person knows to be unauthorised, with the intent of impairing the operation of any computer, preventing or hindering access to any program or the data held in any computer, impairing the operation of any program or the reliability of any data, or enabling any of the above. On indictment, the maximum penalty is 10 years' imprisonment. In 2017 and 2019, two individuals were each sentenced to 16 months in youth offender institutions for separate denial-of-service attacks against various websites targeting websites of law enforcement and a number of companies including Amazon, Netflix and NatWest.

Phishing
Yes. See the answer in respect of hacking.

Under the Fraud Act 2006, phishing could also constitute fraud by false representation if (for example) an email was sent falsely representing that it was sent by a legitimate firm. On indictment, the maximum penalty is 10 years' imprisonment. In 2021, a text scammer was found guilty of fraud by false representation after sending bulk text messages to members of the public seeking to deceive recipients into providing personal financial information. The messages included SMS messages claiming to be from the UK HMRC offering grants in relation to the COVID-19 pandemic.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Yes. See the answer in respect of denial-of-service attacks.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Yes. Under the Computer Misuse Act 1990, it is an offence to make, adapt, supply or offer to supply any article intending it to be used to commit, or that may be likely to be used to commit, an offence under section 1 (see the answer in respect of hacking) or section 3 (see the answer in respect of denial-of-service attacks) of the Act. On indictment, the maximum penalty is two years' imprisonment.

Under the Fraud Act 2006, it is an offence to make or supply articles for use in the course of, or in connection with fraud, provided the individual either: (i) has knowledge that the article is designed or adapted for use in the course of or in connection with fraud; or (ii) intends the article to be used to commit or assist in the commission of fraud. On indictment, the maximum penalty is 10 years' imprisonment.

In 2019, an individual was sentenced to nine years' imprisonment after he created website scripts designed to look like the websites of up to 53 UK-based companies to help criminals defraud victims out of approximately £41.6 million. He also supplied the criminals with software that disguised their phishing sites from being identified by web browsers.

Possession or use of hardware, software or other tools used to commit cybercrime
Yes. See the response relating to the distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime above.

Identity theft or identity fraud (e.g. in connection with access devices)
Yes. Under the Fraud Act 2006, it is an offence to dishonestly make a false representation, knowing that the representation was or may be untrue or misleading, with the intent of making a gain for yourself or another or causing a loss or risk of loss to another (i.e. fraud by false representation). On indictment, the maximum penalty is 10 years' imprisonment. In 2019, an individual was convicted of offences under the Fraud Act 2006 and Computer Misuse Act 1990 (after accessing a barrister colleague's email account to copy his practising certificate in order to produce a faked copy in his own name before going on to practise as a barrister working on 18 cases) and was sentenced to a total of two years' and three months' imprisonment. In 2021, an individual was sentenced to two years' imprisonment after being convicted of fraud by false representation and unauthorised computer access with intent, after using compromised national lottery login details in an attempt to access user accounts to obtain account holders' bank details.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Yes. This may constitute an offence under the Computer Misuse Act 1990 (such as hacking) as well as a financial crime, such as theft (under the Theft Act 1990). A breach of confidence or misuse of private information is actionable as a common law tort, but not as a criminal offence in itself. In 2020, a self-employed IT support specialist was sentenced to 20 months' imprisonment for offences under the Computer Misuse Act 1990 and the Theft Act 1990 after he stole over £31,000 in cryptocurrency from a client.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Yes. See "Hacking (i.e. unauthorised access)" above.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Please see above. In addition, certain terrorism offences may arise in relation to cybersecurity. For example, under the Terrorism Act 2000, it is an offence to take any action designed to seriously interfere with or seriously disrupt an electronic system if this is designed to influence the government or intimidate the public or a section of the public, or for the purpose of advancing a political, religious, racial or ideological cause.

The Data Protection Act 2018 also creates the offence of knowingly, recklessly or without the consent of the controller, obtaining (and retaining), disclosing or procuring personal data. It is also an offence to sell or offer to sell such personal data. These offences are punishable on conviction to a fine.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes. For certain offences under the Computer Misuse Act 1990 (such as hacking, phishing or denial-of-service attacks), the offence will be committed where there is a "significant link to the domestic jurisdiction". This includes the person committing the offence being in the UK, the target computer being in the UK or a UK national committing the offence while outside the UK (provided in the latter instance that the act was still an offence in the country where it took place).

The Data Protection Act 2018 applies to any processing of personal data relating to an individual in the UK by a controller or processor that is not established in the UK, but that offers goods or services, or monitors the behaviour of these individuals in the UK. The offences under the Data Protection Act 2018 can therefore be committed by a legal or natural person outside the UK if they process personal data relating to individuals within the UK in order to target those individuals.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

There is an exemption for certain offences under the Computer Misuse Act 1990 (such as hacking, phishing or denial-of-service attacks) in respect of an enforcement officer acting in accordance with legislation to facilitate inspection, search or seizure without a person's consent. There are no general defences under the Computer Misuse Act 1990. However, Crown Prosecutors will consider a number of public interest factors before charging an individual with an offence.

In relation to the offence under the Data Protection Act 2018 outlined above, it is a defence if the person can demonstrate that obtaining, disclosing, procuring or retaining data without the controller's consent was necessary for the purposes of preventing or detecting crime, required or authorised by law or order, or justified in the public interest. There are other defences available relating to the person's reasonable belief or special purpose (e.g. if they acted in the reasonable belief they had a legal right, or had the controller's consent, or acted for a special purpose).

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

England and Wales does not have a comprehensive cybersecurity law; instead, the legal framework for cybersecurity is dispersed across a number of different laws:

- **The Data Protection Act 2018 –** applies, alongside the EU General Data Protection Regulation, as it forms part of the laws of England and Wales, Scotland and Northern Ireland by virtue of the **European Union (Withdrawal) Act 2018** (**UK GDPR**), to Incidents to the extent that they involve Personal Data. The Data Protection Act 2018 also sets out data protection requirements for national security and immigration as well as other domestic areas of law.
- **The Communications Act 2003 –** includes cybersecurity obligations that apply in the telecommunications sector to public electronic communications network providers and public electronic communications service providers.
- **The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) –** includes security obligations in respect of personal data that apply to public electronic communications service providers.

- **The Network and Information Systems Regulations 2018 (NIS Regulations) –** impose obligations on operators of essential services (**OES**) and relevant digital service providers (**RDSPs**). OES are organisations that operate services deemed critical to the economy and wider society such as water, transport, energy, healthcare and digital infrastructure. RDSPs are anyone who provides online marketplaces, online search engines or cloud computing services and, is a medium or large-sized business with its head office, or a nominated representative in the UK. The NIS Regulations require OES and RDSPs to have sufficient security systems in place to prevent the data they hold or the services they provide being compromised and to report certain Incidents to a competent authority. The ICO is the competent authority for RDSPs. See question 2.2 below for more information about OES.
- **The Regulation of Investigatory Powers Act 2000 (RIPA) –** governs certain investigative powers of law enforcement, such as surveillance and interception of communications data.
- **The IPA 2016 –** amends the RIPA, provides for additional investigative powers, and creates criminal offences of the unlawful interception of communications, subject to limited exceptions for legitimate business purposes.
- **The Computer Misuse Act 1990 –** sets out various cybercrime offences, though does not define what is meant by a "computer" (see the answers to question 1.1 above), which may be prosecuted in conjunction with offences under the **Theft Act 1968**, **Theft Act 1978**, **Criminal Law Act 1977**, **Proceeds of Crime Act 2002**, or the **Fraud Act 2006**.
- **Official Secrets Act 1989 –** may apply in respect of servants of the Crown or UK government contractors, and creates offences in relation to disclosure (or failure to secure) certain information that may be damaging to the UK's interests.
- Governance obligations, which can directly or indirectly relate to cybersecurity, apply to public companies under the **Companies Act 2006**, the Disclosure Guidance and Transparency Rules and the Listing Rules in the **Financial Conduct Authority (FCA) Handbook** and the risk management and control provisions in the **UK Corporate Governance Code**.
- Copyright infringement, including unauthorised copying of documents and the cyber piracy of films, music, e-books, is an offence under the **Copyright Designs and Patents Act 1988**. To the extent an individual seeks to sell counterfeit goods online, the **Trade Marks Act 1994** and **Forgery and Counterfeiting Act 1981** may also apply alongside the Fraud Act 2006 and Proceeds of Crime Act 2002.
- **The Malicious Communications Act 1988 –** sets out criminal offences in relation to malicious and offensive communications, including if the intention is to cause distress or anxiety, or to convey a threat or information that is false (and was known or believed to have been false by the sender).
- Various common law doctrines may also apply in respect of civil actions (see question 5.1 below).

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

- **Telecommunications sector –** cybersecurity requirements under the Communications Act 2003 require providers of public electronic communications networks and public electronic communications services to, amongst other things, maintain the security and integrity of those networks and services, including by taking measures to prevent or minimise the impact of Incidents on end users and on the interconnection of networks.
- **OES/RSDPs –** the NIS Regulations came into force in the UK on 10 May 2018, and impose certain security duties, on any OES and RSDPs, including a duty to notify Incidents to the relevant competent authority. The NIS Regulations require OES and RDSPs to identify and take appropriate and proportionate measures to manage the risks posed, including to prevent and minimise the impact of incidents and to ensure service continuity.
  The NIS Regulations identify sector-based competent authorities (for operators of essential services operating in sectors covering energy, transport, health, drinking water supply and distribution and digital infrastructure) and the ICO is the competent authority for RDSPs. The National Cyber Security Centre (**NCSC**) is the UK's single point of contact for Incident reporting. The NCSC does not have a regulatory function but it undertakes the role of the Computer Security Incident Response Team responding to Incidents that arise as a result of a cyber-attack and that have been notified to it.
  The NIS Regulations introduce a range of penalties that can be imposed by the relevant competent authority. These range from £1 million for any contravention of the NIS Regulations, which the relevant authority determines could not cause an Incident, up to £17 million for a material contravention of the NIS Regulations, which the relevant authority determines has caused, or could cause, an Incident resulting in immediate threat to life or significant adverse impact on the UK economy.
- **Financial services sector –** The Senior Management Arrangements Systems and Controls (**SYSC**) part of the FCA Handbook (see the answer to question 3.2 below) applies to financial services infrastructure providers who are regulated by the FCA – these organisations will be operators of essential services for the purposes of the NIS Regulations (see above).

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the Data Protection Act 2018 (and the UK GDPR), if an organisation processes personal data – information relating to a living individual who can be identified directly or indirectly from that information – it will be required to implement appropriate technical and organisational measures to ensure a level of security of that personal data appropriate to the risk, including the risk of accidental or unlawful disclosure of, or access to, that personal data. The UK GDPR explicitly identifies, as part of these measures, ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services, and the ability to restore the availability and access to personal data in a timely manner in the event of an Incident.

Under the Data Protection Act 2018 and UK GDPR, controllers (i.e. the natural or legal persons that determine how and why personal data is processed) are also required to document any personal data breaches, and (depending on the circumstances) report certain personal data breaches to the ICO or individuals whose personal data is affected (see questions 2.4 and 2.5 below). Where an organisation reports a personal data breach to the ICO, it must describe the measures taken or proposed to be taken to address the personal data breach including measures to mitigate possible adverse effects.

The NIS Regulations also require operators of essential services and digital service providers to take appropriate and proportionate technical and organisational risk management measures, including to prevent and minimise the impact of Incidents.

Under the PECR, a public electronic communications service provider must take appropriate technical and organisational measures to safeguard the security of its service and maintain a record of all Incidents involving a personal data breach in an inventory or log. This must contain the facts surrounding the breach, the effects of the breach and the remedial action taken by the service provider.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

The Data Protection Act 2018 and UK GDPR

Under the Data Protection Act 2018 and the UK GDPR, a controller will be required to notify an Incident involving personal data to the ICO without undue delay and, where feasible, within 72 hours after becoming aware of it, unless it is unlikely to result in risks to individuals. This notification must include: (a) a description of the nature of the Incident; (b) the name and contact details of the organisation's data protection officer or contact point; (c) the likely consequences of the Incident; and (d) the measures taken, or proposed to be taken, to address the Incident and mitigate possible adverse effects.

Under the Data Protection Act 2018, the ICO is not permitted to publicise any information that has been disclosed to it (e.g. through notification of an Incident) if that information relates to an identified or identifiable individual or business and is not already in the public domain. However, this restriction on publication will not apply in certain cases, such as if the ICO determines that publication is in the public interest. The ICO's practice is not to publicise data breach notification information unless it has taken public enforcement action in relation to the breach, or publication is necessary in the public interest (e.g. to allay public concern).

The NIS Regulations

The NIS Regulations also require OES and RDSPs to report Incidents to the relevant competent authority without undue delay. The relevant authority may inform the public where public awareness is needed either to prevent or resolve the Incident, or where this would otherwise be in the public interest, but the organisation will be consulted before disclosure to the public is made to preserve confidentiality and commercial interests.

The NCSC publishes a weekly threat report on its website, with content drawn from recent open source reporting, which details cyber threat information, known network and software vulnerabilities and other information organisations and individuals may find useful. However, there is no obligation for organisations to report threat information to the NCSC to compile these reports.

The Communications Act 2003

The Communications Act 2003 requires public electronic communications network providers to notify Ofcom of any breach of security that has a significant impact on the network's operation. It also requires public electronic communications service providers to notify Ofcom of any breach of security that has a significant impact on the operation of the service.

PECR

The PECR requires a public electronic communications service provider to notify the ICO of a data breach within 24 hours of becoming aware of the "essential facts" of the breach. The notification must include: (a) the service provider's name and contact details; (b) the date and time of the breach (or an estimate) and the date and time of detection; (c) information about the nature of the breach; and (d) the nature and content of the personal data concerned and the security measures applied to it.

The FCA and PRA Handbooks

An organisation regulated by the FCA are also required to notify the FCA of any significant failure in its systems and controls under Chapter 15.3 of the Supervision Manual of the FCA and PRA Handbooks, which may include Incidents that involve data loss. Similarly, the FCA expects payment service providers to comply with European Banking Authority guidelines on major Incident reporting under which those providers are expected to report major operational or security Incidents to the competent authority within four hours from the moment the Incident was first detected, with intermediate updates and a final report delivered within two weeks after business is deemed to have returned to normal.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Under the Data Protection Act 2018 and the UK GDPR, a controller will be required to notify affected individuals of an Incident without undue delay if the Incident involves personal data and is likely to result in a high risk to the rights and freedoms of those individuals. This notification must include: (a) a description of the nature of the Incident; (b) contact details where more information can be found; (c) the likely consequences of the Incident; and (d) the measures taken, or proposed to be taken, by the organisation to address the Incident and mitigate possible adverse effects.

Under the PECR, a public electronic communications service provider must notify its affected subscribers or users of an Incident without unnecessary delay if that Incident is likely to adversely affect their personal data or privacy. The service provider should provide a summary of the Incident, including the estimated date of the breach, the nature and content of personal data affected, the likely effect on the individual, any measures taken to address the Incident and information as to how the individual can mitigate any possible adverse impact. No notification is required if the service provider can demonstrate to the ICO's satisfaction that the personal data that has been breached was encrypted or was rendered unintelligible by similar security measures.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

- The **ICO** is the relevant regulator under data protection laws, including the Data Protection Act 2018, the UK GDPR and the PECR, as well as the competent authority for RDSPs under the NIS Regulations (https://ico.org.uk/).
- **Ofcom** is the relevant regulator under the Communications Act 2003 (https://www.ofcom.org.uk/).
- The **FCA** is the relevant regulator under the FCA Handbook (https://www.fca.org.uk/). The **PRA** is also responsible for the regulation and supervision of financial services firms.
- **Sector-based competent authorities** are the relevant regulators in Schedule 1 to the NIS Regulations (https://www.legislation.gov.uk/uksi/2018/506/schedule/1/made).

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

- **The Data Protection Act 2018 and the UK GDPR** – failure to report an Incident involving a personal data breach can incur a fine of up to the higher of 2% of total annual worldwide turnover or £8.7 million (other infringements of the UK GDPR can incur fines of up to the higher of 4% of total annual worldwide turnover or £17.5 million).
- **The PECR –** failure by a public electronic communications service provider to notify an Incident involving a personal data breach to the ICO can incur a £1,000 fixed fine. A failure by a public electronic communications service provider to take appropriate technical and organisational measures to safeguard the security of their service can incur a fine of up to £500,000 from the ICO.
- **The NIS Regulations –** failure to comply with the NIS Regulations by RDSPs, depending on the type of contravention, can incur a monetary penalty of up to £17 million (for material contraventions that could or have caused an incident that results in a threat to life or significant adverse economic impact to the UK).
- **The IPA 2016** creates civil liability for unlawful interception and provides a civil sanctions regime under which the Investigatory Powers Commissioner can issue a penalty notice of up to £50,000 (where the person has not committed the criminal offence).

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In July 2019, in the first fine to be announced by the ICO under the UK GDPR, the ICO announced an intention to issue a fine of £183.39 million to British Airways, following an Incident in September 2018. This fine was later revised to £20 million in October 2020, to reflect certain mitigating factors (including the remedial measures taken by British Airways in response to the Incident, British Airways' cooperation with the ICO, the lack of aggravating factors, and the impact of the COVID-19 pandemic). The Incident in part involved the unauthorised access of British Airway's IT systems (via the compromised credentials of a user within a third-party supplier, specifically a remote-access account that was not subject to multi-factor authentication) and the diversion of user traffic to the British Airways website to a fraudulent site. Through this false site, customer details were harvested by the attackers. Personal data of approximately 429,000 customers was compromised in this Incident, which is believed to have begun in June 2018. In the detailed penalty notice published in October 2016, the ICO indicates that the fine was imposed due to a failure to ensure appropriate data security, and a failure to use and implement appropriate technical and organisational security measures.

Also, in July 2019, the ICO announced an intention to fine Marriott International £99.2 million, following a data breach affecting Marriott subsidiary Starwood's guest reservation database. This fine was later revised to £18.4 million in October 2020 to reflect certain mitigating factors (including Marriott's steps to mitigate the effects of the Incident, cooperation with the ICO, and the impact of the COVID-19 pandemic on Marriott). A variety of personal data (including guest name and identifier, gender, date of birth, contact details, passport data, credit card data, and loyalty programme information) contained in approximately 339 million guest records globally were exposed by the Incident, of which 7 million related to UK residents. It is believed the relevant vulnerability began in 2014 (prior to Marriott's acquisition), but was not discovered until 2018 (by which time Marriott had acquired Starwood). The Incident involved the installation of a "web shell" on the Starwood network, which allowed the implementation of remote-access Trojan malware to enable remote administration of the system. The ICO found that Marriott failed to undertake sufficient due diligence when it bought the Starwood hotels group in 2016, and should have done more to secure its systems. In the detailed penalty notice published in October 2020, the ICO identifies four principal failures: (i) insufficient monitoring of privileged accounts; (ii) insufficient monitoring of databases; (iii) insufficient control of critical systems; and (iv) insufficient encryption.

In November 2020, the ICO issued a fine of £1.25 million to Ticketmaster UK Limited following a data breach involving an attack on a third-party-hosted chat-bot on its online payment page. The Incident allowed the harvesting of customer financial data and affected 9.4 million customers in the EEA, including 1.5 million located in the UK (which was a member of the EEA at the time of the Incident). In the detailed penalty notice, the ICO identifies failures to assess the risks of using a chat-bot on a payment page, implement appropriate security measures to negate such risks, and identify the source of suggested fraudulent activity promptly, despite warnings.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

There are no specific laws prohibiting the use of web beacons in the UK. However, where use of a web beacon involves processing personal data, the organisation's use of the web beacon must be in accordance with the requirements of the PECR and data protection laws.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

There are no specific laws prohibiting the use of honeypots in the UK.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There are no specific laws prohibiting the use of sinkholes in the UK.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Monitoring of employees, e.g. monitoring use of email and internet access, involves processing of personal data and so the Data Protection Act 2018 and the UK GDPR apply. The ICO's Employment Practices Code (the **Code**) contains guidance on monitoring employees at work. Though the Code was produced under previous legislation, the ICO has confirmed that it considers the information useful (the ICO is also currently conducting a public consultation on its guidance for employment practices). The Code states that employees have an expectation of privacy, and so monitoring should be justified, proportionate, secured and that organisations should undertake an impact assessment and ensure that the employees are notified that monitoring will take place. A failure to comply with the Code will not automatically result in a breach of the UK GDPR or the Data Protection Act 2018. However, an organisation should be able to justify any departure from the Code, and the ICO can take this into account when considering enforcement action.

Under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, an organisation may lawfully monitor and record communications without consent to: (a) ascertain compliance with regulatory practices or procedures relevant to the business; (b) ascertain or demonstrate standards that ought to be achieved by employees using the telecommunications system; (c) prevent or detect crime; (d) investigate or detect unauthorised use of the telecommunications system (such as detecting a potential Incident); and (e) ensure the effective operation of the telecommunications system.

It is not an offence to intercept communications under the IPA 2016 if the person has lawful authority and has the right to control the system (for example, an employer in relation to a private communications system) or has consent of such person to carry out the interception (for example, is authorised IT personnel acting on the employer's instructions). The IPA 2016 is supplemented by the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018, which allows for the lawful interception, monitoring and recording of communications by businesses in limited circumstances. These regulations require the business to demonstrate a permitted purpose of interception (as outlined in the regulations), which includes investigating or detecting unauthorised use of the system or any other telecommunication system. The system controller must have made all reasonable efforts to inform individuals who use the system that their communications may be intercepted.

The Human Rights Act 1998 and, in particular, the right to respect for private and family life, home and correspondence, must also be considered and balanced against obligations on the organisation to implement appropriate security measures in respect of potential Incidents.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

There are no specific restrictions on the import or export of commercial technology designed to prevent or mitigate the impact of cyber-attacks.

However, export authorisations may be required for the export of certain technology that can be used for both civil and military purposes under the Council Regulation (EC) No 428/2009 of 5 May 2009 (as retained and amended pursuant to the European Union (Withdrawal) Act 2018). This could, amongst other things, include information security systems, equipment and components that contain or employ encryption and decryption technology.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Certain sectors, such as financial services and telecommunications, are more incentivised to avoid the cost and reputational impact of Incidents. In some organisations, cybersecurity practice is driven not only by compliance with Applicable Laws but also the desire to promote good "cyber hygiene" culture. For example, although there is no legal requirement to train employees in cyber risks, many organisations do and may carry out simulations (such as phishing simulations and "war games") as a matter of good practice.

Public sector organisations (such as the National Health Service) and government authorities are subject to additional reporting guidelines issued by the central government, in addition to disclosure obligations under Applicable Laws.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Under SYSC 3.2.6R, regulated financial services organisations are required to take reasonable care to establish and maintain effective systems and controls to comply with regulatory requirements and standards and to counter risk that the organisation may be used to further financial crime. Further, under SYSC 3.1.1R, the organisation is required to maintain adequate policies and procedures to ensure compliance with those obligations and countering those risks. These requirements extend to cybersecurity issues. For example, the FCA has previously fined Tesco Bank (£16.4 million) and three HSBC firms (£3 million) for failure to have adequate systems and controls in place to protect customer confidential information and manage financial crime risk.

In the telecommunications sector, public electronic communications network providers and public electronic communications service providers must take appropriate technical and organisational measures to manage risks to the security of the networks and services, including to minimise the impact of Incidents. Public electronic communications network providers must also take all appropriate steps to protect, so far as possible, the availability of that provider's network.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

A failure to prevent, mitigate, manage or respond to an Incident may be a breach of directors' duties if, for example, the failure resulted from a lack of skill, care and diligence on the part of the relevant director. Directors are required, under the Companies Act 2006, to promote the success of the company for the benefit of its members as a whole and exercise reasonable skill, care and diligence in performing their role. It is up to the board of directors of each company to ensure that the board has the relevant competence and integrity to exercise these duties in view of the risk to the company as a whole, including the risk of Incidents.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

No, there are no specific requirements in this respect. However, listed companies are required, under the UK Corporate Governance Code, to set up certain committees with responsibility for specific areas, such as audit. Financial services companies may also be required to have a risk committee. These committees may, as part of their functions, conduct risk assessments that cover cyber risk. The UK Corporate Governance Code emphasises the board's responsibility to determine and assess the principal risks facing the company. This responsibility extends to a robust assessment of the company's emerging risks, which would cover cyber risk.

However, if a company processes personal data, the UK GDPR also imposes an obligation on that company to take appropriate technical and organisational measures (to secure the data) in order to demonstrate compliance with UK GDPR standards. Depending on the nature and context of the data processing, it may be an appropriate technical and organisational measure to conduct periodic cyber-risk assessments and perform penetration or vulnerability assessments. For example the ICO's online guidance on security contains a (non-binding) checklist for companies to assess compliance. At the time of writing, this ICO checklist recommends organisations to: (i) regularly review their information security policies and measures; and (ii) conduct regular testing and reviews of their security measures to ensure they remain effective.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Under the Disclosure Guidance and Transparency Rules set out in the FCA Handbook, listed companies are required to disclose an Incident if the Incident amounts to inside information that may affect the company's share price. For example, theft of business-critical intellectual property is likely to be price-sensitive information.

There are other general annual report requirements that do not explicitly reference cybersecurity but may encourage the reporting of Incidents (depending on the nature of the Incident). For example, as per the Companies Act 2006, the purpose of the strategic report is intended to inform shareholders and help them assess how directors have performed their duty to promote the success of the company (which may include their response to a major Incident).

The UK Corporate Governance Code (applicable to premium listed companies) also requires that the board conducts a robust assessment of the company's emerging and principal risks, and provides a description of its principal risks and an explanation of how such risks are being managed in its annual report. Though cybersecurity is not explicitly referenced, an Incident may be relevant to the annual report if it represents a principal risk to the company.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

There are a number of potential civil actions that may be brought in relation to any Incident, for example:

- Breach of confidence. Where there is unauthorised disclosure or use of information and: (i) the information itself had a necessary quality of confidence about it; (ii) that information was imparted in circumstances importing an obligation of confidence; and (iii) there was an unauthorised use of that information to the detriment of the party communicating it.
- Breach of contract. This could take any form, including a breach of a commercial contract or breach of an employee's terms and conditions of employment. For example, if a party has contractually agreed or warranted that it complies with an ISO standard, a failure to do so will be a breach of contract.
- Breach of trust. A person who owes a fiduciary duty to another may not place him or herself in a situation where they have a personal interest that may conflict with the interest of the person to whom the fiduciary duty is owed. If an Incident is caused by an employee or a director, a breach of trust/fiduciary duty may be claimed. Dishonest assistance may be claimed where there is a fiduciary relationship and dishonest assistance has been given by a third party to the breach of trust.
- Causing loss by unlawful means. A defendant will be liable for causing loss by unlawful means where they intentionally cause loss to the claimant by unlawfully interfering in the freedom of a third party to deal with the claimant.
- Compensation for breach of the Data Protection Act 2018 (and UK GDPR). Individuals who suffer "material or non-material damage" by reason of any contravention, by a data controller, of any requirements of the Data Protection Act 2018 (including the UK GDPR) are entitled to compensation for that damage. "Non-material damage" includes distress. This does not require the claimant to prove pecuniary loss.
- Conspiracy. The economic tort of conspiracy requires there to be two or more perpetrators who are legal persons who conspire to do an unlawful act, or to a lawful act but by unlawful means.
- Conversion. The tort of conversion may cover unauthorised interference with personal information and other property.

- Deceit. There are four elements: (i) the defendant makes a false representation to the claimant; (ii) the defendant knows that the representation is false or is reckless as to whether it is true of false; (iii) the defendant intends that the claimant should act in reliance on it; and (iv) the claimant does act in reliance of the representation and suffers loss as a consequence.
- Directors' duties. See the answer to question 4.1 above.
- Infringement of copyright and/or database rights. Copyright is infringed when a person, without authority, carries out an infringing act under the Copyright, Designs and Patents Act 1988, such as copying the work or communicating the work to the public. Database rights are infringed if a person extracts or re-utilises all or a substantial part of a database without the owner's permission.
- Misuse of private information. Similar to a breach of confidence, but removing the need for the claimant to establish a relationship of confidence. The cause of action may be better described as a right to informational privacy and to control dissemination of information about one's private life.
- Negligence may be claimed where the defendant owed a duty of care to the claimant, breached that duty of care and that breach caused the claimant to suffer a recoverable loss.
- Trespass is the intentional or negligent interference with personal goods. A deliberate attempt through the internet unlawfully to manipulate data on a computer may amount to trespass to that computer.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

The following are illustrations of cases that have been brought that can be said to relate to Incidents.

Breach of confidence and various economic torts

Ashton Investments Ltd v OJSC Russian Aluminium (Rusal) [2006] EWHC 2545 (Comm): there was a good arguable case justifying service out of the jurisdiction, in respect of claims for breach of confidence, unlawful interference with business, and conspiracy where a computer server in London had allegedly been improperly accessed from Russia and confidential information and privileged information had been viewed and downloaded.

Contract

Bristol Groundschool Ltd v Intelligent Data Capture Ltd [2014] EWHC 2145 (Ch): a contract relating to the development of computer-based pilot training materials was a "relational" contract containing an implied duty of good faith. One party had behaved in a commercially unacceptable manner in accessing the other party's computer and downloading information, but its conduct was not repudiatory.

Frontier Systems Ltd (t/a Voiceflex) v Frip Finishing Ltd [2014] EWHC 1907 (TCC): an internet telephony provider's customer whose computer network had been hacked was not liable to pay the bill incurred by unauthorised third parties.

Trespass

Arqiva Ltd & Ors v Everything Everywhere Ltd & Ors [2011] EWHC 1411 (TCC): obiter reference to Clerk & Lindsell on Torts (20th Edition) at paragraphs 19-02 and 17-131. At paragraph 19-02, the authors state the proposition that "one who has the right of entry upon another's land and acts in excess of his right or after his right has expired, is a trespasser". At paragraphs 17–131, the authors refer to "Cyber-trespass" and say that "[w]hile the definition of corporeal personal property may normally be straightforward, questions may nevertheless arise in a number of borderline cases, in particular in respect of electronic technology. For example, it is hard to see why a deliberate attempt through the internet unlawfully to manipulate data on a computer should not amount to trespass to that computer".

Compensation for breach of the Data Protection Act 2018 (and UK GDPR)

Wm Morrisons Supermarket PLC v Various Claimants [2020] UKSC 12: although determined under previous legislation, in the first group litigation data breach case to come before the courts, Morrisons Supermarket was, following an appeal, found not to be vicariously liable for a deliberate data breach carried out by a rogue employee, out of working hours and at home on a personal computer. The ICO had, separately, concluded an investigation into the data breach and found that Morrisons had discharged its own obligations as required under the Data Protection Act 1998 and common law. At first instance, the court concluded that Morrisons had no primary liability in respect of the breach, but there was nonetheless a sufficient connection (as the rogue employee accessed the data in question in the course of his employment) for Morrisons to have vicarious liability. However, this position was overturned on appeal to the Supreme Court.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Please see the list in response to question 5.1 above.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limitations.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Law enforcement authorities have various surveillance powers under UK laws. For example, the Police Act 1997 authorises covert entry into and interference with communications systems by the police, and similar powers are available to the security services under the Security Service Act 1989 and the Intelligence Services Act 1994.

Other powers of surveillance and interception of communications data are subject to the IPA 2016 and RIPA. For example, the IPA 2016 allows certain public authorities to issue targeted interception warrants, bulk interception warrants, targeted

examination warrants, and mutual assistance warrants. Targeted interception warrants can authorise any activity by authorised public bodies for obtaining secondary data and can compel private bodies (including telecommunications operators) to assist public authorities in conducting intelligence-gathering activities. Certain warrants under the IPA 2016 require dual ministerial and judicial approval, or (in addition), Prime Ministerial approval.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

The RIPA, as amended by the IPA 2016, empowers public authorities to require disclosure of a decryption key to enable it to access – i.e. put into an accessible form – encrypted electronic material in its possession (where it has obtained such information lawfully) or where it is likely to obtain such electronic information lawfully. The relevant authorised public bodies can: (i) require disclosure of protected information in an intelligible form; (ii) require disclosure of the means to access the protection information; (iii) require the means of putting protected information into an intelligible form; and (iv) compel the person disclosing to secrecy (to prevent tipping-off). The powers extend to electronic data, which without the decryption, cannot (or cannot readily) be accessed or placed into an intelligible form.

Demands for an encryption key under the RIPA (as amended by the IPA 2016) are subject to judicial authorisation, or a warrant issued by the Secretary of State or judge, or authorisations under the Police Act 1997. Authorised public bodies can also seek encryption key demands via a targeted equipment interference warrant under the IPA 2016.

The IPA 2016 – as supplemented by the Investigatory Powers (Technical Capability) Regulations 2018 (SI 2018/353) – allows the Secretary of State to place obligations on telecommunications operators (or postal operators) to install permanent interception capabilities through "technical capability notices" (**TCN**). The purpose of a TCN is to ensure that when a warrant is served, or an authorisation or notice given, the company can give effect to it securely and quickly.

Nigel Parker is a partner specialising in intellectual property, data protection and privacy, commercial contracts and IT law. He is a member of the firm's Cyber Security Group and has advised clients on strategies for managing legal risk in relation to cybersecurity, including the deployment of a variety of risk management tools, on the response to attacks and dealing with regulatory authorities, and on taking pro-active steps in response to attacks.
Nigel is recognised in *Chambers* and *The Legal 500*. He was named one of the "Top 40 under 40" data lawyers by *Global Data Review*.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 3136
Email: nigel.parker@allenovery.com
URL: www.allenovery.com

Benjamin Scrace is an associate specialising in data protection, commercial contracts, cybersecurity and IT law. He advises clients on advisory and transactional data protection and e-privacy matters, and the negotiation of complex commercial arrangements. Benjamin has previously spent time on secondment with a multinational electronics and technology company supporting the global data protection office.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 1125
Email: benjamin.scrace@allenovery.com
URL: www.allenovery.com

Allen & Overy is a full-service global elite law firm headquartered in London. Our commitment to help our clients deliver their global strategies has seen us build a truly global network now spanning over 40 offices. We have also developed strong ties with relationship law firms in more than 100 countries where we do not have a presence.
We have a strong cybersecurity practice comprising a core team of 19 partners with diverse backgrounds in data protection, bank regulation, anti-trust, securities laws, technology, IT, litigation, employment, IP and corporate. This spread is crucial because cybersecurity Incidents frequently span a wide range of traditional legal practice areas. There is an important legal component to cybersecurity and our integrated team of diverse practitioners reflects this requirement. As a full-service global elite law firm, we are able to advise clients on all legal issues concerning cybersecurity.

www.allenovery.com

ALLEN & OVERY

France

BERSAY

Frédéric Lecomte

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking is a criminal offence pursuant to article 323-1 of the French Criminal Code ("**FCC**") relating to unauthorised access to an automated data processing system. The punishment for fraudulent access into an automated data processing system is imprisonment and a fine of up to €60,000. When data is modified or suppressed as a result of the unauthorised access, the sanction is three years of imprisonment and a fine of up to €100,000. When the offence is committed in a public or governmental system, the sanction is raised to five years of imprisonment and a fine of up to €150,000.

Denial-of-service attacks
Article 323-2 of the FCC sanctions the impeding or slowing down of an information system. Any kind of obstruction falling within the perimeter of article 323-2 is punishable by five years of imprisonment and a fine of up to €150,000. When the offence involves a public or governmental system, the sanctions are raised to seven years of imprisonment and a fine of up to €300,000.

Phishing
Phishing is sanctioned by the following articles of the FCC and of the Intellectual Property Code: (i) the collection of data by fraudulent, unfair or unlawful methods is sanctioned by article 226-18 of the FCC with five years of imprisonment and a fine of up to €300,000; (ii) the theft and use of a third-party identity is sanctioned by article 226-4-1 of the FCC by one year of imprisonment and a fine of up to €15,000 – the applied sanction is cumulative with the sanctions applied pursuant to (i) above; (iii) fraud or swindling is sanctioned by article 313-1 of the FCC with five years of imprisonment and a fine up to €375,000; (iv) unauthorised introduction of data in a system, the extraction, reproduction, transmission and use of data stored in this system is sanctioned by article 323-3 of the FCC with five years of imprisonment and a fine of up to €150,000; and (v) phishing can result in an infringement of intellectual property rights, in particular on the basis of articles L.335-2, L.713-2 and L.713-3 of the French Intellectual Property Code. The owner of the reproduced or imitated website or trademark can sue the phisher for the use of his trademark on the basis of infringement. This offence is sanctioned with three years of imprisonment and a fine of up to €300,000.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
This offence can by sentenced pursuant to article 323-1 of the FCC (*see Hacking*) but also pursuant to article 323-2 of the FCC (*see Denial-of-service attacks*) and pursuant to article 323-3 of the FCC (*see Phishing*).

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
(*See Possession or use of hardware.*)

Possession or use of hardware, software or other tools used to commit cybercrime
Pursuant to article 323-3-1 of the FCC, the act consisting of, without a legitimate motive (in particular for research or computer security), importing, holding, offering, transferring or making available equipment, instruments, computer programs or any data designed or specially adapted to commit one or more offences mentioned in articles 323-1 to 323-3 of the FCC (*see Hacking, Denial-of-service attacks and Phishing*) is punished with the most severe sanctions.

Identity theft or identity fraud (e.g. in connection with access devices)
Pursuant to article 226-4-1 of the FCC, the act of usurping the identity of a third party is punishable by one year of imprisonment and a fine of up to €15,000.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
The offence of theft pursuant to the FCC (article 311-1) has been extended to computer theft by French courts. French judges now consider computer data (i.e. dematerialised information), as constituting goods likely to be stolen.

Under French law, theft is punishable by three years of imprisonment and a fine of up to €45,000.

Article 226-18 of the FCC, as well as articles L.335-2, L.713-2 and L.713-3 of the French Intellectual Property Code (*see Phishing*), could also be used in some circumstances.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Insofar as the owner of the IT is not aware of or has not authorised the penetration testing, this could be punished as hacking or a denial-of-service attack (*see Hacking, Denial-of-service attacks*).

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Article L.66 of the French Post and Electronic Communications Code imposes sanctions of two years of imprisonment and a fine of up to €3,750 for any person who, by breaking wires, damaging equipment or by any other means, deliberately interrupts electronic communications.

Attacks on the fundamental interests of the nation committed by means of information technologies are punished by numerous provisions of the FCC. For example, pursuant to article L.413-10 of the FCC, the destruction, misappropriation, subtraction, reproduction of the defence secrecy or the giving of access to an unauthorised person or making it available to the public, is sentenced to seven years of imprisonment and a fine of up to €100,000.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Pursuant to article 113-2-1 to the FCC, any crime or offence committed by means of an electronic communication network is deemed to have been committed on the territory of the Republic when it is attempted or committed to the detriment of a natural person residing in the territory of the Republic or a legal person whose registered office is in France.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Article L.2321-4 of the Defence Code provides protection to any "ethical hacker" who informs the French National Cybersecurity Agency ("**ANSSI**") of the existence of a vulnerability concerning the security of an automated data processing security. The ANSSI notifies the relevant organisation while protecting the confidentiality of the identity of the person who reported the vulnerability. Moreover, an offence will only be sanctioned by a court pursuant to the FCC if the intentional nature of the offence results from the facts or is demonstrated by the prosecutor. Pursuant to the GDPR as applied under French law, the lack of intentional motivation, all measures taken by the controller or the processor to mitigate the damage suffered by the data subjects, and/or the degree of cooperation to remedy the breach are considered positive behaviour and may reduce the level of administrative sanctions.

2 Cybersecurity Laws

2.1 Applicable Law: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The most important laws in the cybersecurity domain are (without being exhaustive):

- The Godfrain Law (*n°88-19 of January 15, 1988*).
- *Loi Informatique et Libertés n°78-17 of January 6, 1978* ("FDPA") successively amended by two laws: Law *n° 2004-575 of June 21, 2004* and finally amended by *Law n°2018-793 of June 20, 2018* transposing the GDPR and the ordinance *n°2018-1125 of December 12, 2018*.
- The Law for a Digital Republic *n°2016-1321 of October 7, 2016* amended by the law transposing the GDPR (*Law n°2018-493 of June 20, 2018*).
- The Network and Information Systems Security Act ("**NIS Act**") transposing the NIS Directive *n°2018-133 of February 26, 2018* completed by Decree *n°2018-384 of May 23, 2018*, which details the application of the NIS Act and lists the sectors, types of operators and critical infrastructures concerned, and the Decree of September 14, 2018 defining the security rules (together, the "**NIS Rules**").

In addition to the above-mentioned law, the following texts have adapted the criminal law to certain forms of cybercrime and created specific investigative means such as:

- The Law on Daily Security (known as LSQ *n°2001-1062 of November 15, 2001*), the Law on Internal Security (*n°2003-239 of March 18, 2003*).
- The Law adapting the judiciary to developments in crime (*n°2004-204 of March 9, 2004*), the Law on Copyright in the Information Society (known as *DADVSI's Law of August 1, 2006, n°2006-961*).
- The Law OPSI II (*n°2011-267 of March 14, 2011*).
- The Law strengthening the provisions on the fight against terrorism (*n°2014-1353, of November 13, 2014*).
- The Law strengthening the fight against organised crime and terrorism (*n°2016-731, of June 3, 2016*).

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

In France, critical infrastructures identified as such by the law (*Law n°2013-1168 of December 18, 2013, Law n°2016-41 of January 26, 2016, NIS Act*) must comply with specific legal requirements. This is mostly the case for the following infrastructures:

- Professionals subject to the obligation of professional secrecy. For instance, pursuant to article 1111-8-2 of the French Public Health Code, healthcare institutions as well as bodies and services carrying out prevention, diagnosis or care activities shall report without delay serious information system security Incidents to the Regional Health Agency.
- Operators for essential services ("**OES**") that, pursuant to the NIS Rules, are designated by the Prime Minister in various sectors, such as Energy, Transportation, Banking, Financial Markets Infrastructures, Health and Digital Infrastructures. In that regard, the French NIS Rules added specific sectors to the list defined in the Directive such as: insurance; pharmaceutical retailing; and collective catering. The OES shall be designated by an order of the Prime Minister. The OES shall appoint a representative that will be the point of contact of the ANSSI. By November 2018, France had already identified 122 OES.
- Digital service providers ("**DSP**"). Pursuant to the NIS Rules, these infrastructures must appoint a representative established on the national territory of the ANSSI if it is established outside the European Union and does not have any representative within the European Union.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Pursuant to the GDPR, the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the identified risk.

Pursuant to article 57 of the FDPA, the controller (and processor) are required to take all necessary precautions, having regard to the nature of the data and the risks associated with the processing, to preserve the security of the data and, in particular, to prevent it from being distorted, damaged or accessed by unauthorised third parties.

The NIS Rules also require OES and DSP to:

- carry out and maintain a list of networks and information systems necessary for the provision of the essential/digital services;
- identify the risks threatening the security of the information systems;
- guarantee an appropriate level of security according to the existing risks and implement technical and organisational measures necessary and proportionate to prevent, manage and reduce these risks;
- avoid Incidents and minimise their impact so as to guarantee the continuity of their services; and
- identify the IT security risks that may affect their activities.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

The GDPR (article 33) provides for an obligation for all data controllers to notify any Incidents to the competent data controlling body unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. This notification to the data protection authority ("**CNIL**") must take place within 72 hours of the discovery breach, must contain a description of the Incident, an indication of the category of the affected data, the concerned data subjects, a detailed description of the measures taken to remedy or mitigate negative effects, the name and contact details of the data protection officer ("**DPO**"), and must describe possible harmful consequences of the unlawful access and measures taken by the controller.

The FDPA (article 83) specifically concerns DSP and provides for an obligation to notify any data breach to the CNIL immediately and without conditions. The information to be communicated is rather similar to the above mentioned.

The NIS Rules also require OES and DSP to notify the ANSSI "without undue delay" any Incident when it has or is *likely to have* a significant impact on the continuity of services.

As regards the reporting procedures, organisations must provide the ANSSI by electronic means or by mail, with an Incident reporting form available on its website. This form includes information on the reporter, the network information system affected by the Incident, the consequences of the Incident on the services concerned, the type of Incident, its causes and the measures taken to respond to it.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Pursuant to the GDPR and the FDPA, a controller must inform each affected individual of an Incident if the breach may create a high risk to the rights and freedoms of affected individuals (articles 58 of the FDPA and 34 GDPR).

The information must detail the name and contact details of the DPO and describe in clear and plain language (i) the nature of the Incident, (ii) the likely consequences of the Incident, and (iii) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Pursuant to NSI Rules, OES and DSP only are required to report Incidents to the ANSSI.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The CNIL controls the proper application of the FDPA and the GDPR by data controllers and processors. It also gives opinions on legislative drafts or regulatory texts. The CNIL has important powers of control and investigation.

Finally, the CNIL has significant administrative and financial penalty powers and can take decisions such as the temporary or permanent suspension of data processing.

For application of the NIS Rules, the ANSSI is the national authority responsible for responding to cybersecurity Incidents targeting strategically important institutions (https://www.ssi.gouv.fr).

The Ministry of Defence and the Ministry of the Interior also assume functions of prevention of all forms of cybercrime.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Depending on the nature of the offence, the penalty may vary between €10 million or 2% of the worldwide turnover, and €20 million or 4% of the worldwide turnover.

OES and DSP may be subject to the following fines:

- €100,000 (€75,000 for DSP) in case of non-compliance with security rules.
- €75,000 (€50,000 for DSP) in case of failure to communicate a cybersecurity Incident.
- €125,000 (€100,000 for DSP) in case of obstruction of inspection operations.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Since the entry into force of the GDPR, the CNIL has sanctioned several companies. The CNIL fined Google LLC €50 million for lack of transparency, unsatisfactory information and lack of valid consent for the customisation of advertising.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Insofar as beacons have the same purposes, and are deemed to be cookies, their use is legal provided such use complies with cookie legislation.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Under French law, loyalty of evidence production is material to the fairness of trial. Therefore, the law distinguishes between active and passive provocation to commit an offence. Honeypots should be considered legal if used as passive traps to detect cyber threats. The French Cour de Cassation in a decision of April 30, 2014 stated that there had been no provocation to commit the offence in a case where the FBI had created a surveillance site to gather evidence of the commission of credit card fraud.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Operating a sinkhole may not be compliant with the GDPR obligations insofar as some personal data could be collected without the consent of the computer's user and sent to the sinkhole. There is also a risk of collateral damage.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

The CNIL considers the monitoring of employees is possible. The employer can control and limit the use of the internet (site filtering devices, virus detection, etc.) and email (tools for measuring the frequency of messages sent and/or the size of messages, "anti-spam" filters, etc.) provided that (i) prior information and consultation of the employee representative committee has been carried out, and (ii) employees have been individually informed. The monitoring must be proportionate, i.e. respect the balance between the employee's privacy and the employer's power of control.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

In France, encryption media are subject to specific regulations. The use of a means of cryptology is unregulated. However, the sale, supply, import, intra-community transfer and export of an encryption medium are subject, except in listed cases, to a declaration or a request for authorisation depending on the technical functionalities of the means and the planned commercial operation. Decree *n° 2007-663 of May 2, 2007* lists which technology is subject to the declaration or authorisation process. The supplier is responsible for carrying out the declaration or request for authorisation with the ANSSI.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The measures to be implemented are stronger in some business areas. This is particularly the case for critical infrastructures that must comply with the NIS Rules (see question 2.2), or for infrastructures that process sensitive data (for example, health data or data relating to criminal sentences, offences or security measures). Also, as mentioned above (see question 2.2), companies who host personal health data must be accredited for this purpose.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

The legal requirements related to cybersecurity in the following two sectors are as follows:

(a) The financial services sector must comply with several requirements such as auditing IT systems, strengthening resistance to cyber risks, developing defences adapted to the complexity of cyber-attacks, and making several declarations to the ANSSI (ministerial orders of November 28, 2016).

(b) Pursuant to article L.33-1 of the French Post and Electronic Communications Code, companies in the telecommunication sector must comply with rules relating to the conditions of permanence, quality, availability, security and integrity of the network and service, which include obligations to notify to the competent authority breaches to the security or integrity of networks and services.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Beyond the company's responsibility in case of failure of the IT system, the company manager (in France, it is the representative of the company who has the power to bind the company,

e.g.: president; CEO; and general manager) is liable under civil law towards the company and its shareholders of (i) breach of the laws and regulations or of the bylaws, and (ii) mismanagement (article 1850 of the Civil Code). Moreover, the company manager can be liable because of the behaviour of his employees if such behaviour results in damage to a third party (article 1242 paragraph 5 of the French Civil Code). Finally, pursuant to the FCC and the French Commercial Code, numerous French provisions specifically make the company manager subject to personal criminal liability.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Please see below the Applicable Law requirements:

(a) There are no general obligations, so far, to designate a CISO. However, the GDPR sets out the obligation to appoint a DPO when (i) the data processing is carried out by a public authority or public body, (ii) the data processing requires regular and systematic monitoring on a large scale, and (iii) in cases of large-scale processing of sensitive data.

(b) For critical infrastructures, the NIS Rules set out the obligation to establish, maintain and implement a network and information system security policy ("**ISSP**"). The ISSP describes all procedures and organisational and technical means implemented by the operator to ensure the security of its essential information systems. The operator shall also maintain a crisis management procedure in the event of major cyber-attacks. For other companies, there are no general obligations to establish a written Incident response plan or policy.

(c) For critical infrastructures, the NIS Rules requires the OES to carry out and maintain a risk analysis of its essential information systems. Pursuant to the FDPA, the controller and the processor must carry out a risk assessment in order to implement measures to protect data processing systems. Moreover, pursuant to article 1110-4-1 of the French Public Health Code, health professionals, healthcare institutions and services must use information systems for the processing of health data, their storage on electronic media and their transmission by electronic means, in accordance with interoperability and security standards in order to guarantee the quality and confidentiality of personal health data and their protection.

(d) For critical infrastructures, the NIS Rules impose audits to assess the level of security of information systems with regard to known threats and vulnerabilities. For other companies, French law strictly applies the GDPR according to which the controller and the processor must implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (article 32.1.d).

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Pursuant to article L.225-100-1 of the French Commercial Code and article 222-3 of the General Regulations of the French Financial Markets Authority, listed and private companies must draw up an annual management report that contains a description of the main risks and uncertainties the company had to face or is facing (which implicitly includes cyber risks). Pursuant to article L.451-1-2 of the French Monetary and Financial Code, listed companies are required to submit this report to the French Financial Markets Authority and to publish it on their website.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Under French law, the general rule of civil liability is set forth under article 1240 of the French Civil Code, pursuant to which any act that causes damage to another shall oblige the person by whose fault it occurred to repair it (i.e. three elements are necessary to engage liability: (i) a fault; (ii) a damage; and (iii) a causal link between the two). Moreover, under the GDPR (article 79), a civil action may be brought in the event of an Incident if the controller or the processor have not complied with the GDPR requirements. Finally, under the FDPA, the data subject shall have the right to mandate a not-for-profit body, organisation or association to stop the breach and to obtain compensation (article 37).

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

For example, a woman was penalised in civil and criminal terms by the Chambéry Court of Appeal on November 16, 2016 for the possession of hacking data.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

See the answers to questions 6.1 and 6.2 above.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Cyber risk is partially covered by traditional insurance contracts that cover certain foreseeable consequences of certain computer threats (e.g. insurance contracts covering damage to property and civil liability). The emergence of new risks from the evolution of technologies and the increase in their uses requires the implementation of appropriate legal frameworks. To cope with these new risks, insurers have developed a new contract: the cyber contract, which is a multi-risk contract cover for damage (costs and losses incurred), liability (non-material damage to third parties), and management services of crises.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Pursuant to article L.113-1 of the French Insurance Code, the insurer does not cover loss or damage resulting from the

insured's intentional or wilful misconduct. In addition, criminal sanctions are not insurable because they are regarded as personal sanctions. Moreover, there is still a debate about the possibility to insure administrative or financial sanctions to the extent they are not the result of intentional misconducts. The authors opine that this risk should be insurable.

On the subject of terrorism and cyberterrorism, the French Public Purse stated that "insurance contracts whose purpose is to guarantee the payment of a ransom to Daech, as to any terrorist entity, are prohibited".

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

In France, there are many police services specialising in cybersecurity. For example: the PICyAN (cybercrime investigation platform and digital analysis), which analyses IT equipment seized during police searches and internet surveillance thanks to special software; the Digital Crime Centre ("**C3N**"), whose mission includes judicial investigations and criminal intelligence; the Information Technology Fraud Investigation Brigade ("**BEFTI**"), which operates only in Paris and the surrounding suburbs and which is responsible for managing any breaches of the data processing system, software counterfeiting and classic offences such as fraud; and the Central Office for the Fight against Information and Communication Technologies Crime ("**OCLCTIC**"), which ensures the legality of published content on the internet and ordering providers to remove illegal content.

The police services mentioned above may carry out investigations, searches, interceptions, data collection, geolocation, wiretapping, infiltration, and arrest and detain suspects in police custody.

In addition, in order to ensure the effective application of the FDPA, the CNIL has the power to carry out extensive controls on all data controllers and processors. The ANSSI can also carry out controls on OES's facilities.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There is no obligation to set up backdoors. However, the administrative and judicial authorities may require the submission of encryption keys. Pursuant to article L.871-1 of the French Internal Security Code, natural or legal persons who provide encryption services aimed at ensuring a confidentiality function are required to submit within 72 hours to authorised agents (i.e. administrative and judicial authorities), at their request, agreements enabling the decryption of data transformed by means of the services they have provided.

Frédéric Lecomte has been a member of the Paris Bar since 1989. After having spent five years at Coudert Brothers in Paris and 26 years at Stehlin & Associés, Frederic recently joined Bersay as a partner of the IT/IP team.
Frédéric is the author of numerous articles in relation to technology law and is the author of a book about the GDPR, "*Nouvelle Donne Pour les Données*" (Fauve Editions, 2018).
Practice areas: new technologies and data law; intellectual property; contract law; and commercial and distribution law.

BERSAY
31 avenue Hoche
Paris, 75008
France

Tel: +33 1 56 88 30 00
Email: flecomte@bersay.com
URL: www.bersay.com

BERSAY was created in 1995 to meet the essential needs of SMEs in France and abroad. Since then, major groups have been drawn to BERSAY, owing to its pragmatic outlook to help resolve business and legal issues.
The 40 attorneys and legal experts of BERSAY work together in order to offer strategic expertise spanning the main aspects of the life of a company. All of their work has an international component and they are regularly recognised in leading French and international rankings (*Leaders League*, *Best Lawyers*, *The Legal 500*, etc.).
BERSAY has several regional "desks", covering Israel, Japan and French-speaking African countries.
BERSAY is driven by strong values: quality/responsiveness; team spirit; tenacity; and ethics. In 2019, BERSAY won the first "Equality Trophy" from the Paris Bar, and the "Ethics and Diversity Gold Trophy" in 2020 (*Décideurs Magazine*). As the first Parisian law firm to be ISO 9001-certified, BERSAY has built, and regularly adapts, its internal quality processes to respond to the clients' needs and increase its efficiency.

www.bersay.com

Germany

Eversheds Sutherland


Dr. Alexander Niethammer


Dr. David Rieks


Stefan Saerbeck


Constantin Herfurth

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking constitutes a criminal offence according to Sec. 202a and Sec. 202b of the German Criminal Code (so-called "data espionage", Sec. 202a, and "phishing" Sec. 202b). According to Sec. 202a, whosoever unlawfully obtains data for himself, or another, that was not intended for him and was especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine. According to Sec. 202b, whoever, without being authorised to do so, intercepts data that are not intended for them, either for themselves or another, by technical means from non-public data transmission or from an electromagnetic broadcast from a data-processing facility, incurs a penalty of imprisonment for a term not exceeding two years or a fine, unless the offence is subject to a more severe penalty under other provisions. Depending on the facts of the case, "hacking" could possibly come under the definition of both of the offences set out above, depending on the level of protection applied to the data in question.

Denial-of-service attacks
Denial-of-service attacks constitute a criminal offence according to Sec. 303b of the German Criminal Code (so-called "computer sabotage"). According to this provision, whosoever interferes with data-processing operations that are of substantial importance to another by deleting, suppressing, rendering unusable or altering data, or by entering or transmitting data with the intention of causing damage to another, shall be liable to imprisonment for up to three years or a fine. The same applies to destroying, damaging, rendering unusable, removing or altering a data-processing system or data carrier. Also, it is important to note that the sole attempt is punishable and if the data-processing operation is of substantial importance for another's business or enterprise, or a public authority, the penalty can be imprisonment for up to five years or a fine.

Phishing
Phishing can constitute two different criminal offences. The unlawful interception of data by technical means from a non-public data-processing facility constitutes a criminal offence according to Sec. 202b of the German Criminal Code and is punishable with imprisonment for up to two years or a fine. The use of such data with the intent of obtaining an unlawful material benefit would constitute a criminal offence under Sec. 263a of the German Criminal Code (so-called "computer fraud") and is punishable with imprisonment for up to five years or a fine. In especially serious cases of computer fraud, the penalty is imprisonment for a term not exceeding five years or a fine. Furthermore, storing or modifying such data in a way that a counterfeit or falsified document would be created, may constitute a criminal offence under Sec. 269 of the German Criminal Code (so-called "forgery of technical records").

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infection of IT systems with malware constitutes a criminal offence according to Sec. 303b of the German Criminal Code (so-called "computer sabotage"). According to this provision, whosoever interferes with data-processing operations that are of substantial importance to another by deleting, suppressing, rendering unusable or altering data, or by entering or transmitting data with the intention of causing damage to another, shall be liable to imprisonment for up to three years or a fine. The same applies to destroying, damaging, rendering unusable, removing or altering a data-processing system or data carrier. Also, it is important to note that the sole attempt to commit such an offence is punishable. Moreover, if the data-processing operation is of substantial importance to another's business or enterprise, or a public authority, the penalty can be imprisonment for up to five years or a fine.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
According to Sec. 27 of the German Criminal Code, anyone who assists another person in committing an intentional, unlawful act is liable for prosecution (so-called "aiding"). In this context, aiding is provided by the person who physically or psychologically assists another in the intentional commission of an unlawful act.

If someone distributes or sells hardware, software or other instruments being used to commit cybercrime and this use is covered by the seller's intent, then he is liable for the respective completed offence (e.g. see above) in connection with Sec. 27 of the German Criminal Code. The penalty for the aider is based on punishment for the offender. However, the penalty must be mitigated pursuant to Sec. 49 (1) of the German Criminal Code.

Depending on the individual circumstances of the case, assisting an offender could also fall under the definition of abetting (Sec. 26 of the German Criminal Code) if the assistant intentionally induces another to intentionally commit an

unlawful act. In this case, the abettor faces the same threat of punishment as the offender. However, individual punishment may differ from the sentence the offender will receive.

Whenever there is preparatory conduct to data espionage and phishing, Sec. 202c of the German Criminal Code must be considered in particular. This criminal offence was expressly created with a view to the increasing danger of cybercrime and it is supposed to closing gaps in criminal liability prior to actual cyber-attacks. The criminal offence includes the manufacture, sale and procurement for the purpose of using, distributing or otherwise making available a device, including computer programs, which were primarily designed or prepared for the purpose of committing certain cyberattacks. Further, Sec. 202c of the German Criminal Code will be especially applicable for such conduct in which prosecution is not able to prove that the offender or another has committed the criminal offences of data espionage or phishing, but has taken preparatory measures to commit such offences.

Possession or use of hardware, software or other tools used to commit cybercrime

The sole possession of hardware, software or other tools that can be used to commit cybercrime can constitute a criminal offence according to Sec. 202c of the German Criminal Code. According to this provision, the preparation of the commission of data espionage or phishing by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible software for the purpose of the commission of such an offence shall be liable to imprisonment for up to one year or a fine. In case of a use of such instruments, the same principles as set forth above with respect to "Hacking" apply.

Identity theft or identity fraud (e.g. in connection with access devices)

Identity theft can constitute various criminal offences, depending on how the offender obtains access to the identity data. This can either be done by phishing methods, which would constitute a criminal offence under Sec. 202b of the German Criminal Code, as set forth above with respect to "Phishing", or by use of such identity data for fraudulent purposes, which could constitute a criminal offence under Sec. 263 of the German Criminal Code (fraud) or Sec. 263a of the German Criminal Code (computer fraud), both offences being subjected to imprisonment for up to five years, or even up to 10 years in especially serious cases. Depending on the individual facts of the case, the use of such identity of another may further constitute a criminal offence under Sec. 267 (forgery of documents) or Sec. 269 (forgery of data of probative value) of the German Criminal Code, with both offences being punishable by imprisonment for up to five years, or even up to 10 years in especially serious cases.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Electronic theft constitutes a criminal offence under the preconditions of Sec. 202a of the German Criminal Code. Therefore, the affected data must be especially protected against unauthorised access and the offender must gain access to the data by circumventing access protection. Usually, this is not the case when a current or former employee breaches confidence, as the employee has authorised access to the data. However, such conduct may constitute a criminal offence according to Sec. 23 of the German Trade Secret Protection Act (so-called "betrayal of business and corporate secrets") or Sec. 142 of the German Patent Act. Furthermore, such conduct may constitute the criminal offence of "phishing". The above-mentioned principles apply.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Penetration tests are a comprehensive security check of IT infrastructure. It involves taking measures that even a hostile hacker would use to penetrate networks without authorisation.

In Germany, penetration tests may only be carried out with the prior consent of the owner of the IT infrastructure to be tested. Also, with regard to Sec. 202a of the German Criminal Code, a criminal liability is only excluded here if the penetration test is authorised by the owner of the IT infrastructure to be tested.

In addition, even in the case of legal penetration tests, the data protection regulations must be guaranteed at all times, as the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik – "BSI"*) has expressly determined.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Under German criminal law, some other activities in connection with the above-mentioned conduct constitute criminal offences. These are: (i) preparing of an unauthorised obtaining or interception of data, Sec. 202c of the German Criminal Code; (ii) handling of stolen data, Sec. 202d of the German Criminal Code; (iii) violation of postal and telecommunications secrets, Sec. 206 of the German Criminal Code; (iv) computer sabotage, Sec. 303b of the German Criminal Code; (v) certain types of violation of the EU General Data Protection Regulation ("GDPR" (*Datenschutz-Grundverordnung*)) with the intention of enrichment or to harm someone, Art. 84 of the GDPR and Sec. 42 of the German Federal Data Protection Act (*Bundesdatenschutzgesetz*); and (vi) falsification of digital evidence, Sec. 269 *et seq.* of the German Criminal Code.

1.2 Do any of the above-mentioned offences have extraterritorial application?

In general, the application of the German Criminal Code depends on the "place of commission of the offence". According to Sec. 9 of the German Criminal Code, an offence is deemed to have been committed in every place where the offender acted or in which the result occurs, or should have occurred, according to the intention of the offender. Therefore, the above-mentioned offences will be applicable both if the offender acted in the territory of Germany and in case the offence affects IT systems that are situated or used for services provided in Germany where the offender acted from outside Germany. With regard to Sec. 23 of the German Trade Secret Protection Act (so-called "betrayal of business and corporate secrets"), Sec. 5 of the German Criminal Code stipulates extraterritorial application. According to Sec. 5 no. 7 of the German Criminal Code, German criminal law applies regardless of which law is applicable at the place where the offence was committed to a violation of the business or trade secrets of a business that is physically located within the territorial scope of this statute, of an enterprise that has its seat therein, or of an enterprise that has its seat abroad and is dependent on an enterprise that has its seat within the territorial scope of this statute and forms a corporate group with the latter.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Even "ethical hacking" remains a violation of Sec. 202a of the

German Criminal Code, as long as unauthorised action is taken and no prior consent of the IT system owner has been obtained.

In general, under German law, a penalty for criminal or administrative wrongdoing is determined by the degree of individual guilt. There is a margin of discretion for the judge to impose penalties. Positive behaviour after a violation of a statutory provision, as well as compensation for the occurred damage, affect the level of penalties. Therefore, the circumstances of each individual case must be considered. In particular, the subjective circumstances and attitudes as well as the objectives of the offender are also decisive.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Cybersecurity is about to gain considerable momentum, especially amongst companies handling critical infrastructure, as the latest amendments of the German IT Security Act 2.0 (*IT-Sicherheitsgesetz* 2.0) of 28 May 2021, which have amended or complemented a number of laws, now foresee a fine for non-compliance of up to EUR 20 million (see question 2.7 above), much like the GDPR. In general, Cybersecurity is governed by several Acts in Germany. The main legal acts relating to cybersecurity are the GDPR, the Federal Data Protection Act, and the Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik – "BSIG"*). Further, sector-specific parts of cybersecurity are governed for example by the Telemedia Act (*Telemediengesetz*), the Telecommunications Act (*Telekommunikationsgesetz*), the Banking Act (*Kreditwesengesetz*), the Energy Industry Act (*Energiewirtschaftsgesetz*) and the Securities Trading Act (*Wertpapierhandelsgesetz*). Besides this formal legislation, there are a few important informal provisions with respect to IT security in Germany. These are the BSI IT Baseline Protection Manual, which was developed by the BSI, the Common Criteria for Information Technology Security Evaluation, standardised as ISO/IEC 15408 and information security in ISO/IEC 2700, and the Control Objectives for Information and Related Technology ("COBIT"). Furthermore, the European Cybersecurity Act provides the necessary authority to the European Union Agency for Cybersecurity ("ENISA") in order to establish a cybersecurity certification. Companies may voluntarily obtain such certification that is meant to inform the public about IT security provisions and general compliance with relevant IT security regulations. The ENISA will perform cybersecurity training during which companies may evaluate their processes when being subject to a cyber-attack. Generally, the ENISA will be a principal contact for any cybersecurity-related questions. Additionally, the European Commission's first draft of a worldwide first artificial intelligence (AI) act aims to support the development and use of AI in Europe within a secure legal framework. Binding laws for the interaction of cybersecurity and AI technology will follow in the next few years on a national and European level.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Yes, the BSIG provides for specific obligations for critical infrastructure. Critical Infrastructures shall mean facilities, equipment or parts thereof which:

1. are part of the energy, information technology and telecommunications, transportation and traffic, health, water, nutrition, finance and insurance industry sectors; and
2. are of high importance to the functioning of the community as their failure or impairment would result in material shortages of supply or dangers to public safety.

The second amendment to the regulation (*BSI-KritisV, Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz*) that comes into force on 1 January 2022 has extended the list of critical infrastructures by lowering many of the qualifying thresholds. The extensive list by now includes amongst other businesses point of sale terminals, hospitals, data centres, banking and securities, and derivatives transactions.

Operators of Critical Infrastructures must:

- take appropriate organisational and technical precautionary measures to avoid disruptions of the availability, integrity, authenticity and confidentiality of their information technology systems, or any components or processes that are integral to the functionality of the critical infrastructures by implementing the state of the art security measures, recently reinforced by Sec. 8a (1), (1a) of the BSIG;
- demonstrate and provide evidence of compliance with the requirements of the BSI by means of security audits, reviews or certifications at least every two years towards the BSI;
- register with the BSI and notify authorities, as well as specify a contact point to the BSI within six months who must be available 24/7; and
- immediately report the certain Incidents to the BSI via the contact person.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes, German and European law provide for several obligations for organisations to take measures to monitor, detect, prevent and mitigate Incidents.

In detail:

- According to Sec. 13 (7) of the Telemedia Act, telemedia providers must ensure through technical and organisational measures that no unauthorised access to the technical equipment used for their telemedia services is possible and that they are protected against personal data breaches and against disturbances, even if they are caused by external attacks.
- According to Sec. 109 (1) of the Telecommunications Act, providers of telecommunications services must implement technical safeguards to protect telecommunications privacy and personal data and to protect telecommunications and data-processing systems against unauthorised access (further obligations in Sec. 109 (2) to (5) Telecommunications Act).
- Providers of several financial products are obliged to develop an IT-specific risk management (Sec. 25a of the Banking Act and Sec. 80 of the Securities Trading Act).
- According to Art. 5 (1) (f) and Art. 32 of the GDPR, controllers are obliged to process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes, there are specific reporting obligations with respect to Incidents under German and European law.

In detail:

- Controllers must notify personal data breaches to the competent Data Protection Authority under Art. 33 of the GDPR. An exception applies where the security breach is unlikely to result in a high risk to the rights and freedoms of the data subject. The report must be made without undue delay and not later than 72 hours after having become aware of the breach, and must contain a description of the Incident, an indication of the category of the affected data, the concerned data subjects and a detailed description of the measures taken to remedy or mitigate negative effects. The notification to the competent Data Protection Authority must also describe the likely consequences of the personal data breach and the mitigation measures taken by the controller. The name and contact details of the data protection officer must be provided as well.
- Operators of critical infrastructures must notify certain Incidents regarding the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes immediately to the BSI under Sec. 8b of the BSIG. The notification shall include information on the interference, possible cross-border effects and the technical framework, in particular the assumed or actual cause, the information technology concerned, the type of facility or equipment concerned, as well as the critical provided service and the effects of the Incident on this service.
- Providers of public telecommunications networks or services must notify any impairments of telecommunications networks and services that lead or may lead to significant security breaches immediately to the Federal Network Agency and the BSI under Sec. 109 of the Telecommunications Act. The notification must contain information on the impairment, as well as the technical conditions, in particular the presumed or actual cause and the information technology affected.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons (see question 2.4 above), controllers must communicate the personal data breach to the data subject without undue delay under Art. 34 of the GDPR. The communication to the data subject must describe in clear and plain language the nature of the personal data breach and at least contain the information and measures referred to in Art. 33 of the GDPR.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The requirements identified for the above-mentioned requirements are enforced by the BSI, competent Data Protection Authorities and the Federal Network Agency.

In detail:

- The BSI is the main authority with respect to cybersecurity in Germany. This authority should be the main contact regarding questions about preventive security measures and is primarily responsible for receiving notifications about security breaches with respect to critical infrastructures.
- Data Protection Authorities enforce all relevant data protection laws. In Germany, each federal state has a separate Data Protection Authority.
- The Federal Network Agency enforces the telecommunications-related laws and is responsible for receiving notifications about security breaches with respect to telecommunications networks and services.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Sec. 14 of the BSIG (amended by the German IT Security Act 2.0 in connection with Sec. 30 (2) of the Act on Regulatory Offences foresees a fine of between EUR 100,000 to 20 million. Fines could apply if a business belonging to the critical infrastructure does not comply with the requirements or is unable to prove that they did. A fine of up to EUR 1 million for example could be issued if a digital service provider has not taken appropriate and proportionate technical and organisational measures to manage risks to the security of the network and information systems they use to provide digital services within the European Union.

Additionally, under Art. 83 of the GDPR, non-compliance with the aforementioned requirements is subject to fines of up to EUR 10 million or 2% of the worldwide annual turnover, whichever is higher. Depending on the type of data protection infringement, the fine may even be higher.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In light of recent fine regulation by the BSIG, the realisation of these sanctions remains yet to be seen at the time of writing.

German Data Protection Authorities have started imposing administrative fines on companies who have not complied with their obligations under Art. 32 of GDPR. For example, in 2020, the Commissioner of Data Protection and Freedom of Information Baden-Württemberg imposed a fine of EUR 1.24 million on AOK Baden-Württemberg (health insurance) for not processing personal data in a secure manner.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Yes, beacons are permitted.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Yes, honeypots are permitted.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Yes, sinkholes are permitted.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Generally, organisations are permitted to monitor or intercept electronic communications on their networks in order to prevent or mitigate the impact of cyber-attacks. However, at the same time they must comply with applicable data protection laws with regard to the monitoring of electronic communications of its employees, which may lead to certain restrictions.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Germany follows EU regulations and the Wassenaar Arrangement. The export of data encryption products is regulated in Germany by the directly applicable EC Dual-Use Regulation, the Foreign Trade Act (*Außenwirtschaftsgesetz*) and the Foreign Trade Regulation (*Außenwirtschaftsverordnung*). In the recent years, the threat potential of cyber-attacks has grown rapidly. Among other things, the European Union has reacted to this by adapting Annex I of Regulation EC No. 428/2009 ("Dual-Use Regulation") in 2018. The so-called Waassenaar Agreement treats strong cryptography as a weapon of war. Germany has signed this agreement and must therefore monitor the export of certain cryptographic products. Exports of such products are, in principle, subject to a licensing requirement; however, all products that are available in the mass market can be exported without a licence.

There are no import restrictions on data encryption products in Germany, regardless of whether they are hardware or software.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The market practice with respect to information security in Germany mainly depends on the security relevance of the individual business; in particular, whether the sector is considered a sector that is related to critical infrastructures and whether the business processes sensitive personal data or not. However, there are no known sector-specific deviations from the strict legal requirements.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

As financial services and telecommunications can now be considered critical infrastructure, the above-mentioned applies here.

There are also legal requirements as follows:

- Providers of certain financial products are obliged to develop an IT-specific risk management (Sec. 25a of the Banking Act and Sec. 80 of the Securities Trading Act).
- According to Sec. 109 (1) of the Telecommunications Act, providers of telecommunications services must implement technical safeguards to protect telecommunications privacy and personal data and to protect telecommunications and data-processing systems against unauthorised access (further obligations in Sec. 109 (2) to (5) of the Telecommunications Act).

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Yes, such failure may lead to a breach of directors' or officers' duties.

According to Sec. 130 of the German Administrative Offences Act (*Ordnungswidrigkeitengesetz – "OWiG"*), the owner or management of a company commits a misdemeanour if:

- it omits purposefully or negligently to appropriately control the company; and
- if a crime or misdemeanour was committed that could have been avoided or significantly impeded by exercising such control.

The obligation to control also includes the obligation to diligently select and monitor supervising personnel, active monitoring of the development of legal and technical standards, random inspections, enforcement of implementation measures, etc. The owner or management of a company is obligated to organise the company in a manner that allows the company to comply with the law. Consequently, failures to prevent, mitigate, manage or respond to an Incident can constitute a breach of directors' duties if the directors failed to implement the appropriate measures to avoid such occurrences.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Companies that are listed or private may fall under the newly extended criteria of critical infrastructure and therefore may need to register with the BSI. Regarding other businesses, obligations have not been put in place so far to either designate a CISO or equivalent, establish a written Incident response plan or policy or conduct periodic cyber risk assessments. However, according to Art. 32 of the GDPR, such measures can be required in order to ensure appropriate IT security measures. Companies shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In particular, companies shall implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of data processing. This must therefore be assessed on a case-by-case basis. Furthermore, operators of public telecommunications networks or providers of publicly available telecommunications services must appoint a security commissioner under Sec. 109 of the Telecommunications Act.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There are no further obligations beyond the above-mentioned disclosure requirements in the event of data breaches. However, with respect to publicly listed companies, sole cybersecurity risks without an Incident having occurred may trigger the obligation to disclose the cybersecurity risk in an *ad hoc* notification if the risk is likely to have an impact on the company's stock market price.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

If the entity in charge of the attacked IT systems is not reacting appropriately, it is – depending on the kind of Incident – possible to file for an interim injunction of a German court in order to compel such entity to comply with its contractual and statutory obligations. This would require an ongoing Incident, as well as the violation of a statutory or contractual obligation.

Furthermore, it is possible to file for damage payments if the Incident has been enabled by the lack of an appropriate IT security model. In this case, any individual or other company that suffered material damage can take civil actions against the company that is responsible for the Incident. This liability is basically not limited but can be covered by insurance.

Additionally, in terms of private actions, damaging events can often be interrupted or even reversed through close cooperation with law enforcement and compliance departments.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

The case law on Incidents in Germany is very rare due to the lack of the possibility of class actions in Germany. Private actions are usually not published in Germany.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes, civil liability in tort depends on the degree of negligence and the damage that occurred due to the organisation's failure and is basically not limited.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents in Germany.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limitations to insurance coverage against any type of loss.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Depending on the type of authority (e.g. Public Prosecutor, the BSI and Data Protection Authority), the enforcement powers vary. If the conduct being investigated might qualify as a criminal offence, it will be the public prosecution office leading the investigations most commonly using the aid of other authorities. All aforementioned authorities have the power to carry out on-site investigations including accessing IT systems. Furthermore, under certain preconditions according to Sec. 100a of the German Code of Criminal Procedure, telecommunications may be intercepted and recorded without the knowledge of the persons concerned and Sec. 100b of the German Code of Criminal Procedure provides the possibility to gain covert access to information technology systems used by persons concerned. Most recently the German legislator has expanded the scope of application of the aforementioned investigative measures, as from July 2021, for both telecommunications surveillance and covert remote searches of information technologies, the catalogue of potential criminal offences that allow for such investigative measures has been amended. It is therefore expected that the investigative authorities will conduct a higher number of surveillance measures and covert remote searches than in the years before.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No; so far, there is no such obligation. However, the German legislator is currently debating such an obligation with respect to social media and instant messaging accounts. Hence, although the implementation of backdoors or the obligation to provide encryption keys has not yet become existing legislation, it is to be noted that the German legislator makes efforts towards a more transparent cyberworld as, e.g. from February 2022, on the Network Enforcement Act will oblige the operators of large social networks to immediately report certain criminally relevant content – such as threats of murder and rape or child pornography – to the Federal Criminal Police Office (*Bundeskriminalamt – "BKA"*). For this purpose, the provider must have an effective procedure in place that will usually be linked to the corresponding complaints management of the social network. Breaches of the obligation to implement such a procedure will constitute an administrative offence and shall be punishable by a fine of up to 5 million EUR. Furthermore, the German Telemedia Act was amended in April 2021 and now permits providers to pass on personal data as well as the IP address of a user to law enforcement authorities for the prosecution of criminal offences and, to a limited extent, for the prosecution of serious administrative offences in case the provider has been requested to disclose such information to the authorities by a formal request. In cases of particularly serious crimes, providers might also be obliged to hand over their users' passwords.

Acknowledgments

The authors would like to thank Isabella Norbu and Tobias Abersfelder for their contributions to this chapter.

Dr. Alexander Niethammer is Managing Partner of Eversheds Sutherland in Germany. He specialises in cybersecurity, data protection as well as technology transfer and outsourcings, with additional experience in advising on complex IT transactions. With more than 18 years of experience, Alexander has advised many Fortune 100 companies from the IT, industrial, consumer and financial sectors on global projects. He is admitted as an attorney (*Rechtsanwalt*) in Germany and as an attorney-at-law in the State of New York (USA). Alexander is recommended for data protection by *Best Lawyers* and *The Legal 500* and has been recognised as a leading lawyer for both data protection and IT by German business magazine *Wirtschaftswoche*.

Eversheds Sutherland
Brienner Str. 12
80333 Munich
Germany

Tel: +49 89 54565 318
Email: alexanderniethammer@eversheds-sutherland.com
URL: www.eversheds-sutherland.com

Dr. David Rieks is a Partner in the area of compliance and criminal law in the Hamburg office of Eversheds Sutherland. As a certified specialist in criminal law, David advises and represents national and international companies regarding all questions of commercial and tax criminal law. He regularly advises clients with regard to cybercrime and other data breach-related compliance matters. David also helps companies investigate and enforce damage claims resulting from criminal offences or other misconduct by business partners and employees. He is recognised as one of Germany's leading lawyers for white-collar crime by business magazine *Wirtschaftswoche*.

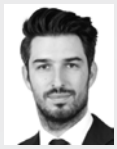
Eversheds Sutherland
Stadthausbrücke 8
20355 Hamburg
Germany

Tel: +49 40 808094 260
Email: davidrieks@eversheds-sutherland.com
URL: www.eversheds-sutherland.com

Stefan Saerbeck is a Principal Associate in the Litigation & Dispute Management practice at Eversheds Sutherland in Munich. Stefan has more than 11 years of experience as a trial lawyer in German courts. He focuses especially on injunction proceedings, as well as regular court proceedings in commercial, corporate and cyber-related disputes. Stefan is a member of the German Institution of Arbitration ("DIS") and the American Bar Association, and a lecturer at the University of the German Armed Forces in Munich. He is recommended as a corporate litigator by *Global Law Experts*.

Eversheds Sutherland
Brienner Str. 12
80333 Munich
Germany

Tel: +49 89 54565 167
Email: stefansaerbeck@eversheds-sutherland.com
URL: www.eversheds-sutherland.com



Constantin Herfurth is an Associate in the Data Protection & Cybersecurity practice at Eversheds Sutherland in Munich. His area of advice covers all aspects of data protection and cybersecurity. In particular, he has strong expertise in the management of data breaches. He mainly advises international and national clients from the industrial and health sectors. Constantin frequently publishes in the specialist journals *Zeitschrift für Datenschutz* (journal for data protection) and *MultiMedia und Recht* (multimedia and law), and is a contributor to the EU chapter of ILO's *Tech, Data, Telecoms & Media* newsletter.

Eversheds Sutherland
Brienner Str. 12
80333 Munich
Germany

Tel: +49 89 54565 295
Email: constantinherfurth@eversheds-sutherland.com
URL: www.eversheds-sutherland.com

As a global top 10 law practice, Eversheds Sutherland provides legal services to a global client base ranging from small and mid-sized businesses to the largest multinationals, acting for 70 of the Fortune 100, 61 of the FTSE 100 and 128 of the Fortune 200.
With more than 3,000 lawyers, Eversheds Sutherland operates in 74 offices in 35 jurisdictions across Africa, Asia, Europe, the Middle East and the United States. In addition, a network of more than 200 related law firms, including formalised alliances in Latin America, Asia Pacific and Africa, provide support around the globe.
In Germany, more than 160 lawyers, tax advisors and notaries in Berlin, Dusseldorf, Hamburg and Munich provide advice to multinational groups, listed and medium-sized companies, investors, financial service providers, as well as family businesses in all relevant areas of commercial and tax law. In the fields of data protection and cybersecurity, the German team in particular provides advice on data security, the reform of the European data protection law, the transfer of data abroad, data protection management, as well as with regard to employee data protection and digitalisation issues such as Big Data, AI and the internet of things. The team, which is part of the global Data Privacy & Cybersecurity Group of Eversheds Sutherland, furthermore advises on data protection management and provides support with regard to crisis management in case of data breaches and cyberattacks.

www.eversheds-sutherland.com

EVERSHEDS SUTHERLAND

Greece


Dr. Nikos Th. Nikolinakos


Dina Th. Kouvelou


Alexis N. Spyropoulos

Nikolinakos & Partners Law Firm

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking, according to the Greek Criminal Code (GCC) is a criminal offence pursuant to Art. 370B par. 1 that applies to unauthorised access to electronic data, and Art. 370D par. 2 of the GCC that applies to unauthorised access to information systems or to information transmitted through telecommunication systems. Under Art. 370B par. 1, hacking carries the penalty of imprisonment up to two years, while under Art. 370D par. 2 of the GCC, hacking carries the penalty of imprisonment from 10 days to five years. If hacking causes a severe hindrance to the operation of an information system or when data is modified or suppressed as a result of hacking, Art. 292B may also apply, in accordance with which the penalty ranges from 10 days to five years of imprisonment depending on the severity of the outcome; it also includes the imposition of a penalty fee.

Pursuant to Art. 15 of Law 3471/2006, which regulates privacy in the field of electronic communications, a penalty fee of €10,000 to €100,000 may be imposed if the offender gained access to personal data of subscribers or users of the system in an unauthorised manner.

Denial-of-service attacks
Denial-of-service attacks constitute a criminal offence under Art. 292B GCC, which sanctions the impeding of an information system's operation, with imprisonment from 10 days up to five years and the imposition of a penalty fee. If a certain tool (e.g. botnet) was used for the attacks, the penalty will be a minimum of one year of imprisonment and a penalty fee; however, if the attack caused severe damage or targeted critical infrastructure, a penalty of at least two years of imprisonment and a penalty fee or three years' imprisonment and a penalty fee applies to each case, respectively (Art. 292B of the GCC par. 2 sec. a, and secs b and c, respectively).

Phishing
When phishing has the meaning of attempting to fraudulently acquire through deception sensitive personal information (such as passwords), it falls under Art. 386 par. 1 of the GCC and bears a penalty of 10 days to five years of imprisonment and a penalty fee.

On the contrary, if phishing is defined as a type of fraud that involves the use of a computer, by creating false digital resources intended to resemble those of legitimate entities, to induce individuals to reveal or disclose sensitive personal information, then it falls under Art. 386A of the GCC par. 1 and bears a penalty of 10 days to five years of imprisonment and a penalty fee.

In both cases, when the damage that occurred as a result of phishing exceeds the amount of €120,000, the penalty is imprisonment of up to 10 years and a penalty fee.

In respect of the above three offences (hacking, denial-of-service and phishing), according to Art. 4 part II of Law 4411/2016: a) a recommendation for compliance; b) an administrative fee from €20,000 to €1,000,000; c) a revocation or suspension of their operating licence; or d) an exclusion from public services may be imposed on the offender if the offence was carried out by a legal person. For the cumulative or selective application of the above administrative sanctions, the imposing authority takes into account the gravity of the offence, the degree of intent, the economic status of the legal entity and any existing offending history.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infection of IT systems with malware is a criminal offence and can be sanctioned pursuant to Arts 292B, 292D, 370A, 370B, 370D par. 2, 370E and 386Ab of the GCC, depending on the type of infection of the IT system.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
These acts constitute criminal offences under Art. 292C of the GCC, bearing a penalty of imprisonment of up to two years or a fine under the condition that the hardware, software or other tools were used to commit the cybercrimes described in Art. 292B of the GCC.

Possession or use of hardware, software or other tools used to commit cybercrime
This offence can be sanctioned pursuant to Art. 292C of the GCC, bearing a penalty of imprisonment of up to two years or

a fine under the condition that the hardware, software or other tools were used to commit the cybercrimes described in Art. 292B of the GCC (as above).

Identity theft or identity fraud (e.g. in connection with access devices)
Pursuant to Art. 386A of the GCC, whoever, with the purpose of gaining illegal profit, damages foreign property by influencing by any means of data processing, faces a penalty of up to 10 years' imprisonment and a penalty fee. Apart from the above-mentioned case, identity theft can constitute several criminal offences under GCC, depending on the manner and reason for which the offender obtains access to the identity data.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Given that electronic theft is not a specific criminal offence under the GCC, Greek courts have considered that: a) under Art. 370C par. 1 of the GCC (state and non-state secrets violation), with a penalty of three months' imprisonment; and b) under Art. 370D of the GCC, if the offender is offering its services to the information system owner (e.g. current employee), the offence is punishable only if it is expressly stated in the bylaws or in a written decision of the owner.

Law 2121/1993 on intellectual property, in its Art. 66, provides for criminal penalties of at least one year's imprisonment and a €2,900 to €15,000 fine for illegal unauthorised copies, reproductions and sale of material that are protected under its provisions. Art. 65 of the same law provides for civil liabilities in case of copyright infringement and Art. 65A for administrative penalties up to €1,000 per copy if someone reproduces or sells illegal copies.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Any unfair – including without permission – violation of elements or programs of computers – such as a software or system intervention in order to determine its vulnerabilities – shall be considered a crime independently pursuant to Art. 370C of the GCC, or as a preparatory action on the occasion of which the above crimes may be committed.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Within the framework of Law 4624/2019 (Art. 38), if anyone who commits the above acts simultaneously intervenes in any way in a system for personal data archiving, and by doing so becomes aware of the data, and: a) copies, removes, changes, damages, collects, adds, organises, saves, adapts, recovers, seeks, correlates, combines, limits, erases, destroys them; or b) transmits, diffuses, or communicates them to non-eligible persons, is sanctioned with imprisonment for up to one or up to five years, respectively. In case any of the above acts concern special categories of personal data (Art. 9(1) of the General Data Protection Regulation (GDPR)) or data relating to criminal convictions and offences (Art. 10 GDPR), the sanction consists of imprisonment for one to five years and a fine of up to €100,000. In case penalties are provided by both the Penal Code and Law 4624/2019, the more severe penalties apply.

Administrative sanctions
In Art. 4 of Law 4411/2016, administrative sanctions are defined against legal entities in favour of which the offences as described above are committed. The sanctions include a) recommendations for compliance, b) an administrative fee from €20,000 to €1,000,000, c) a revocation or suspension of their operating licence, or d) an exclusion from public services, if the hacking has been committed by a legal person. For the cumulative or selective application of the above administrative sanctions, the imposing authority takes into account the gravity of the offence, the level of intent, the economic status of the legal entity and any existing offending history.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The GCC applies for all criminal offences with their "place of the offence" within Greece (Art. 5 par. 1 of the GCC). According to Art. 5 par. 3 of the GCC, when the offence is committed via a network or other means of communication, Greece is also considered the place of offence if, in that territory, specific means for the offence are accessible. The "place of the offence" is defined under Art. 16 par. 1 of the GCC as the place where the offender actually committed the offence, in whole or in part, as well as the place where the result of the offence took or would have taken place.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Most of the crimes described above contain the condition of purpose for their sanctions to apply. For example, in the subjective element of identity theft or identity fraud, the perpetrator of an act is punished when there is the intention of personal (or in favour of a third party) financial gain. As a similar condition, hacking is sanctioned when the perpetrator acts unfairly – a condition that obviously cannot include cases of ethical hacking.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The following laws are the most significant instruments with regard to cybersecurity:

- Law 4727/2020 regarding "Digital Governance (Transposition into Greek Legislation of Directive (EU) 2016/2102 and Directive (EU) 2019/1024) – Electronic Communications (Transposition into Greek Legislation of Directive (EU) 2018/1972) and other provisions".
- Law 4577/2018, which transposed NIS Directive 2016/1148/EU into Greek law, regarding measures for a high common level of security of network and information systems.
- Ministerial Decision No. 1027/2019, issued by the Minister of Digital Governance, which specifies the implementation and the procedures provided under Law 4577/2018.
- The GDPR and the relevant Greek Law 4624/2019.
- Law 4411/2016, which transposed Directive 2013/40/EU into Greek law, on attacks against information systems.
- Law 4070/2012, in relation to the operation of electronic communications networks and the provision of electronic communications services.

- Act 205/2013 of the Hellenic Authority for Communication Security and Privacy (ADAE), which is a Regulation for the Security and Integrity of Networks and Electronic Communication Services.
- Art. 12 of Law 3471/2006, regarding the protection of personal data and privacy in the electronic telecommunications sector and the operators' obligation to take the necessary safety measures.
- Draft Law of the Greek Code of Electronic Communications, which is a transposition of the Directive (EU) 2018/1972 into Greek law.
- Art. 386A of the Greek Penal Code, regarding fraud committed via a computer.
- Law 2121/1993, i.e. the Greek Copyright Act, recently amended and replaced by Art. 25 of Law 4708/2020.
- Law 3674/2008, which concerns the ensuring of telephone communication confidentiality.

Although the following are not legislation *per se*, they are included for reasons of completeness:

- The National Cybersecurity Authority of the Ministry of Digital Governance has issued its National Cybersecurity Strategy for the period 2020–2025.
- The National Cybersecurity Authority has issued a Cybersecurity Handbook regarding best practices for protection and resilience of information systems.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Law 4577/2018 and Ministerial Decision No. 1027/08.10.2019 outline the responsibilities of essential service operators, i.e. critical infrastructure operators in the fields of energy, transportation, banking and finance, health, drinking water and IT infrastructures, which are the following:

- adopting technical and organisational measures to identify potential security risks and to prevent and minimise the impact of cybersecurity Incidents;
- notifying all Incidents that might severely impact the operational continuity of the essential services they are providing to the Hellenic Cybersecurity Authority (HCA) and the Hellenic Cyber Security Incident Response Team (CSIRT) without undue delay;
- collaborating with the competent authorities;
- ensuring that the operator's Security Policy is in line with the Comprehensive Security Policy issued by the HCA and that the "Basic Security Requirements", as outlined by the HCA are adhered to; and
- designating a Chief Information Security Officer (CISO).

According to Law 4577/2018, the HCA, in cooperation with the competent regulatory and oversight authorities, is responsible for identifying essential service operators in Greece and compiling a list of the essential services and their operators, which is updated regularly – every two years at a minimum. It also supervises operator compliance with the provisions of said Law and, in case of severe violation, may impose fines ranging from €15,000 to €200,000.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

There are several legal provisions for organisations to take measures for monitoring, detecting, preventing or mitigating incidents:

- According to Art. 148 of Law 4727/2020, providers of public electronic communications networks or of publicly available electronic communications services take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services. Taking into account the most advanced technical capabilities, those measures shall ensure a level of security appropriate to the risk presented. In particular, measures, including encryption where appropriate, shall be taken to prevent and minimise the impact of security incidents on users and on other networks and services. The above providers notify the ADAE of a security incident that has had a significant impact on the operation of networks or services without undue delay
- Act 205/2013 of the ADAE sets similar obligations for undertakings providing public communications networks or publicly available electronic communications services to take the appropriate technical and organisational measures.
- Along the same lines, Art. 2 of Law 3674/2008 stipulates that providers of electronic communications networks or electronic communications services are responsible for the security of their connections and of the hardware and software systems that they use. To this end, they have the obligation to take the appropriate technical and organisational measures and to use hardware and software systems, which ensure the confidentiality of the communication and allow the revelation of the violation or attempted violation of the confidentiality of the communication. The providers are also obligated to carry out regular controls on the hardware and software systems that are under their supervision and to have full knowledge of their technical possibilities.
- Law 4577/2018 establishes significant obligations for organisations in regard to security measures on their behalf. In particular, operators of essential services and digital service providers shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems that they use in their operations and to prevent and minimise the impact of Incidents affecting the security of the network and information systems used for the provision of their services (Arts 9 and 11).
- According to the GDPR, personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Art. 5(f)). Under Art. 32, the Controller and the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, *inter alia*, as appropriate: the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical Incident; and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- Art. 12 of Law 3471/2006 regarding the protection of personal data and privacy in the field of electronic communications also sets obligations for providers of electronic communications services, as they must take appropriate technical and organisational measures in order to protect the security of the services provided.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Several instruments within the Greek and European legal frameworks require organisations to report information related to Incidents and potential Incidents to the competent authorities.

Art. 33 GDPR provides that "in case of a personal data breach, the Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority", which in this case is the Hellenic Data Protection Authority (HDPA), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The notification must contain the information provided in Art. 33 par. 3 (a–d).

Law 4577/2018 provides that in case an Incident is related to essential service operators (Art. 9(1)(c)) or to digital service providers (Art. 11(1)(c)), the operators and providers are required to notify the HCA and the Hellenic CSIRT without undue delay, and their notification must include all information necessary for the Authorities to assess the critical nature of the Incident and its potential cross-border impacts.

Pursuant to Art. 17(2)(d) of ADAE Decision No. 205/2013 titled "Regulation for the Security and Integrity of Networks and Electronic Communications Services", on the mitigation of Security Incidents, the organisations providing public communications networks or publicly available electronic communications services (providers) must, without undue delay, notify all Incidents jeopardising the security and integrity of networks and services to their Security and Network Integrity Manager and competent executives, as well as to the ADAE, which is the competent authority.

Pursuant to Art. 148(2) providers of public electronic communications networks or of publicly available electronic communications services are required to notify the ADAE without undue delay, with regard to the privacy of a security incident that has had a significant impact on the operation of networks or services; in turn, they will also: a) without undue delay, notify all such security incidents to the HCA; and b) in the event that Incidents affect the availability or integrity of networks or services, notify the Hellenic Telecommunications and Post Commission (EETT). On a case-by-case basis, the ADAE notifies the competent authorities in other Member States and the European Union Agency for Cybersecurity (ENISA).

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Pursuant to Art. 34 GDPR, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall communicate the personal data breach to the data subject without undue delay and shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Art. 33(3). The communication to the data subject is not required if any of the conditions of Art. 34 par. 3 (a–c) are met.

Law 4577/2018 provides that in case an Incident takes place, operators – of essential services (Art. 9 par. 1) and of digital service providers (Art. 11 par. 1) – are required without undue delay to report the Incident to the HCA and the relevant CSIRT. After consultation with the relevant provider, the HCA may inform the public of individual Incidents or require the relevant provider to do so, as far as this is required to prevent a future Incident or to handle an ongoing Incident or if such disclosure is deemed to be in the public interest.

Art. 148 (par. 2) of Law 4727/2020 provides that when faced with a significant security threat, operators of electronic communication services shall inform users of their services, who may be affected by such a threat, of any possible protection measures or remedies that the users can adopt. Where appropriate, providers also inform their users of the threat itself. A similar obligation (i.e. informing the subscribers of an imminent security threat and proposing appropriate measures accompanied with the respective costs) is provided under Art. 12 (par. 2) of Law 3471/2006, which regulates the protection of personal data and privacy in electronic communications along with the GDPR and Law 4624/2019. The aforementioned article also provides that in case of a breach of personal data that may adversely affect the personal data or privacy of the subscriber or a third party, the provider shall promptly inform the affected subscriber or other affected person (Art. 12 par. 6).

Lastly, pursuant to Art. 8 of Law 3674/2008, in case of a breach of confidentiality of communication or a significant threat thereof, the person responsible for ensuring confidentiality is obliged to immediately inform the provider or its legal representative, the prosecutor's office, the ADAE and the affected subscribers.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The competent authorities for the enforcement of the above-mentioned requirements are:

- The HDPA, a constitutionally consolidated independent authority, serves as the watchdog of the personal data and privacy of individuals in accordance with the provisions of Law 4624/2019 and Law 3471/2006. An additional mission of the HDPA is the support and guidance to Controllers in their compliance with the obligations set by the law.
- The EETT, an independent authority granted with specific rights under the Hellenic Constitution, acts as the national regulator of the telecommunications and postal market. It was established in 1992 by virtue of Law 2075/1992; however, several new laws and amendments have expanded its competence. The Laws in force are 4070/2012 (for electronic communications) and 4053/2012 (for postal services market and electronic communication matters).
- The ADAE has been established under Law 3115/2003 and Art. 19 par. 2 of the Hellenic Constitution, having, *inter alia*, the competence to: issue regulations regarding the assurance of the confidentiality of communications; perform audits on communications network/service providers, public entities as well the Hellenic National Intelligence

Service; and hold hearings of the aforementioned entities, to investigate relevant complaints from members of the public and to collect relevant information using special investigative powers.

- The HCA, as designated by Law 4577/2018 implementing the NIS Directive, consists of the Directorate of Cyber Security of the General Secretariat of the Ministry of Digital Policy, Telecommunications and Media (as established by Art. 15 of Decree 82/2017). The HCA monitors, *inter alia*, the implementation of the NIS Directive, cooperates with the Hellenic CSIRT and is designated as the single point of contact to ensure cross-border cooperation with competent authorities of other EU Member States.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

In respect of the GDPR, an administrative fine of up to €10,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year – whichever is higher – may be imposed in cases of non-compliance with the obligations of: a) Controllers and Processors; b) the certification body; and c) the monitoring body as specified under this legal instrument. The aforementioned penalties are doubled in case of infringements of: a) the basic principles for processing, including conditions for consent; b) the data subjects' rights; c) the personal data being transferred to a recipient in a third country or an international organisation; d) the obligations established under national law under Chapter IX of the Regulation; and e) in the case of non-compliance with an order, a temporary or definitive limitation on processing, the suspension of data flows by the supervisory authority or a failure to provide access in violation as all respectively defined. The same penalties may also be imposed in the case of non-compliance with an order issued by the supervisory authority. Art. 39 of Law 4624/2019 enables the HDPA to impose an administrative fine of up to €10,000,000 against the public authorities defined under Law 4270/2014 for a number of specifically designated infringements on the grounds of a relevant specially detailed decision following a prior call for explanations of the interested party for each case at issue. In addition, the HDPA is entitled (Art. 82 of Law 4624/2019) to impose to competent authorities' administrative fines of up to one or €2,000,000 in the specifically designated circumstances where the latter fail to comply with their obligations as personal Data Controllers. Moreover, the national legislator provides criminal sanctions (under Art. 38 of Law 4624/2019) of both imprisonment and penalty payments of €100,000, €200,000 and €300,000 for the offences defined therefor.

Furthermore, the ADAE is entitled to address a recommendation for compliance with a certain provision of the law (being complemented by a warning for the imposition of sanctions in the case where a recurrence of the violation of the law governing the confidentiality of communication or the prerequisites and the procedure related to its declassification is substantiated), while it may also impose an administrative fine ranging from €15,000 to €1,500,000 (Art. 11 of Law 3115/2003).

Fines varying from €20,000 to €5,000,000 may be imposed on telecommunication operators if they fail to comply with the obligations set out in Law 3674/2008. Under Art. 12 of Law 3674/2008, the ADAE, in case of a violation of Art. 2 of said Law, can either impose a fine or set the operator a deadline for compliance. In case of severe violations, the ADAE transfers the file to the EETT, which has the right to impose the suspension or revocation of the right to provide telephony services.

Pursuant to Art. 13 of Law 3471/2006, the HDPA and ADAE may impose fines and other administrative measures in accordance with Art. 11 of Law 3115/2003 and 21 of Law 2472/1997, respectively, in cases of violation of Arts 1–17 of Law 3471/2006. These fines may vary from €880.41 (minimum fine imposed by HDPA) to €1,500,000 (maximum fine imposed by the ADAE).

In addition, should providers of public electronic communications networks or publicly available electronic communications services fail to provide the information necessary to assess the security of their networks and services, including documented security policies to the ADAE or to be subject to its security control or generally to comply with the obligations set out in Art. 148 of Law 4727/2020, the ADAE may impose one of the following penalties: a) a recommendation for compliance within the time limits set by the notice of a fine in the event of non-compliance; and b) a fine from €15,000 to €1,500,000 (under Art. 149 of Law 4727/2020).

Lastly, Law 4577/2018 provides for the competence of the Minister of Digital Governance to impose on a) essential service operators, b) digital service providers, and c) any natural and legal person a number of penalty payments ranging from €15,000 to €200,000 following a relevant recommendation issued by the HCA (Art. 15). These fines are applicable when the aforementioned persons do not notify Incidents entailing a serious impact on the operation of their services or they do so but with undue delay, or in the case where they do not undertake both appropriate and proportionate, technical and organisation measures on a provisional basis to manage the risks related to the security of the networks and information systems used for such services ((a) and (b)). In respect of natural/legal persons in general, the imposition of a fine is related to the non-provision or the provision with undue delay of any relevant information that is required within the context of inspections or Incident investigation.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In 2021, the HDPA had imposed on the grounds of Art. 83 par. 2 GDPR, administrative fines of €2,000 (Decision No. 12/2021), €5,000 (Decision No. 17/2021), €20,000 (Decision No. 13/2021). Within the context of Art. 83, the HDPA has also imposed a fine of €15,000 (Decision No. 23/2021). On the basis of the violation of Art.15 GDPR and Art. 11 of Law 3471/2006, the HDPA imposed a penalty sanction of €2,000 on a candidate member of Parliament (Decision No. 7/2021).

In addition, fines of €2,000 were imposed for the violation of Art. 11 of Law 3471/2006, within the context of Art. 83 of the GDPR to a candidate municipal councillor and to a candidate member of the Parliament (Decisions No. 8 and 19/2021).

Finally, the HDPA imposed the sanction of the administrative fine of €10,000 on the Municipality of Tavros-Moschato for the violation of Arts 5 and 6 pars 1 and 17 par. 1 of the GDPR (Decision No. 21/2021). In particular, the Authority considered that posting documents containing personal data on the webpage of the Ministry of Digital Governance constitutes a form of illegal processing.

It is noteworthy that the imposition of the above fines was determined on an *ad hoc* basis being further qualified as an additional and effective, proportionate and preventive pecuniary sanction, aiming at both bringing into conformity and penalising the unlawful conduct.

With regard to copyright and related rights infringements on the Internet, the Copyright Committee (EDPPI) recently had its role enhanced under the recent amendment of Art. 66E of the

Greek Copyright Act (intended to extend and foster its competency with the aim of rapidly dealing with online infringements), which provides for a supplementary total 15 days' timeframe within which access blocking may be ordered, provided that the circumvention of a decision already issued by the Committee is substantiated. Since the issuing of the first decision under the revised provision is currently pending, it is worth noting to cite the enforcement actions already taken by the Committee; in all cases, EDPPI ordered for the blocking of access to the infringing content for a time period of three years. In relation to the fines imposed on ISPs, the administrative pecuniary sanctions ordered (on the grounds of the respective assessment of the severity of the infringement) are listed as follows: €850 (Decision No. 3/2018); and €700 (Decisions No. 5/2019, 7/2019, 9/2019, 11/2019, 15/2020, 16/2020 and 17/2020) for each day of non-compliance with the operative part of the said decisions.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Greek law does not prohibit the use of beacons for cybersecurity purposes; however, such use would have to be assessed under e-privacy and data protection legislation. Insofar as beacons are regarded as cookies due to the similarity of the purpose for which they are used, their use is legal if it complies with cookie legislation, namely the ePrivacy Directive 2002/58/EC as it was amended in 2009 and transposed into Greek law by Law 3471/2006.

If the use of web beacons results in the processing of personal data (e.g. users' personal account information or their IP addresses, which qualify as personal data if the entity collecting the IP address has the means to identify the person using it), it ought to be in compliance with the provisions of the GDPR.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
The use of honeypots is not prohibited under Greek law.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
The use of sinkholes is not prohibited under Greek law.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Organisations are responsible for preventing and responding to cyberattacks. However, monitoring or intercepting electronic communications on their networks may only be permitted under specific and strict circumstances. Particularly, interception of communications (e.g. calls) falls under the scope of privacy of communications and may not be performed without a prosecutor's order. However, stored communications (e.g. emails) or monitoring of logs in real time to prevent cyberthreats is not considered to fall under the scope of communications privacy, but rather under the provisions of the personal data protection framework. In such case, organisations are required to adhere to the requirements of the GDPR and Law 4624/2019. Such processing of personal data will be considered lawful if it is grounded on the purposes outlined in Art. 6 GDPR, in particular on whether it is deemed necessary for the purposes of the legitimate interests pursued by the organisation acting as a Data Controller. Safeguarding the security of its network system, protecting its property from severe threats and verifying or preventing illegal activity, constitute legitimate interests in order for the organisation to process personal data, on the condition that the measures adopted are appropriate to the risks and organisations have documented detailed and specific justifications with regard to their nature and necessity.

The lawfulness of monitoring network communications also crucially hinges on whether employees are provided with prior, clear and concise information on the collection and processing of their data. In addition, it should be stressed that in accordance with the principle of purpose limitation, if the processing of personal data is conducted specifically in order to ensure the safety of the system or network, such data may not be further processed for other purposes (e.g. to monitor employee performance), while the use of any monitoring system needs to take into account the principles of proportionality and accountability with regard to the collection and storage of employees' personal data.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

On an EU level, Regulation No. 428/2009 governs the EU's export control regime on "dual-use" items, which are broadly defined as items, including software and technology, which can be used for both civil and military purposes. Dual-use items are listed on a common and regularly updated annex, which includes products that use cryptography, such as encryption software and hardware. The Regulation provides that dual-use items, with some exceptions, may be traded freely within the EU, and it imposes common export control rules on Member States, including a common set of assessment criteria and common types of authorisations. Export authorisations are required in order for dual-use items to be exported from an EU Member State to third countries. Decision No. 121837/E3/21837 of the Ministry of Finance was published in 2009, to implement the provisions of Regulation No. 428/2009.

Greece is also member of the Wassenaar Arrangement, which is an agreement between states on the import and export of conventional arms and "dual-use" goods and technologies, including internet-based surveillance systems and software designed to defeat a computer or network's protective measures so as to extract data or information, as well as IP network surveillance systems.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

ISO Certifications, such as ISO/IEC 27001, are a very common market practice in the context of information security in various business sectors, e.g. the telecommunications sector. There are not any known sector-specific deviations from the strict legal requirements.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Organisations both in the financial services (banking and financial market infrastructures) and in telecommunications fall under Laws 4577/2018 and 4411/2016, which establish obligations for security requirements and incident notifications. Moreover, Law 4577/2018 applies these provisions for organisations in the following sectors: energy; transport; health; drinking water supply and distribution; digital infrastructure; and digital service providers. There are some additional provisions related to the telecommunications sector, as mentioned in question 2.3, which emphasise on the need for organisations in the telecommunications sector to take the appropriate technical and organisational measures in order to protect the security of the services they provide (Art. 148 of Law 4727/2020, Act 205/2013 of the ADAE and Art. 12 of Law 3471/2006).

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

There are no provisions in the Greek S.A. Law (Law 4548/2018) stipulating that a failure by a company to prevent, mitigate, manage or respond to an Incident amounts to a breach of directors' or officers' duties, within the meaning of duty as it is set out in Art. 102 of the said Law. However, specific provisions in relation to corporate liability are set in Law 4577/2018, which is sector specific for operators of essential and of digital services.

In particular, Law 4577/2018 provides that the above operators are subject to administrative fines – both at a company and at an individual level (Art. 15) – in case they breach their obligation to notify the competent authority of the Incidents having a significant impact on the continuity of services they provide. The same fines are also applicable in case the above companies do not take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems that they use in their operations as well as in cases where it is confirmed that a natural or legal person does not provide (or provides with undue delay) information requested in the context of an investigation of an Incident.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

According to Decree 1027/8.10.2019, specifying the provisions of Law 4577/2018, operators of essential services and providers of digital services are required to designate a CISO. The Decree requires that the above operators take efficient, effective and proportional measures to address cybersecurity risks but does not indicate how those measures shall be concretised. In that regard, while the law does not explicitly set an obligation to establish an Incident response plan, to conduct periodic cyber risk assessment and to perform penetration or vulnerability tests, it nonetheless implies that those measures shall be adopted by operators for the latter to comply with the law.

In relation to providers of public communication networks or publicly available electronic communications services, Art. 148 of Law 4727/2020 sets upon them the obligation to take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services. Specifically, an Incident response plan obligation is provided for providers of electronic communications services in Art. 17 of Act 205/2013 of the ADAE. The plan includes the following actions: a) recording of details for each Incident; b) figuring out the reasons and the technical/organisational inefficiencies that may have resulted in the incident; c) carrying out certain restoration actions within a certain timeframe; and d) notifying the CISO, competent executives and relevant authorities.

The GDPR, being applicable to all businesses, requires in its Art. 32 that Data Controllers and Data Processors take the appropriate technical measures to comply with the obligation of secure data processing. According to the interpretation of the article, the Incident response plan/policy, the vulnerability assessment and the periodic penetration tests, while also not explicitly laid down within the text of the GDPR and Law 4624/2019, they are nonetheless implicitly included among the necessary measures that Data Controllers or Processors need to take. Finally, as regards the designation of a Data Protection Officer (DPO), Law 4624/2019 requires only public entities to appoint a DPO. While a DPO and a CISO should be in close collaboration, their role is distinct and as such an operational independence must be maintained between these two positions within an entity.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

No further disclosure obligations are stipulated within the Greek legislation, aside from those mentioned in section 2 above.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Art. 40 of Law 4624/2019 – corresponding to Arts 79 and 82 GDPR – provides the right to a judicial remedy, namely a claim for damages, against a Data Controller or Data Processor of any data subject whose rights under the GDPR have been infringed as a result of the processing of his/her data in non-compliance with the GDPR. The infringement of a data subject's rights (Incident) may refer to a hack, or a violation or threat to the confidentiality, integrity and availability of the data subject's personal data that resulted in a material or moral damage to the data subject. Claims for damages by the data subject *vis-à-vis* Controllers or the Processors shall be filed before the court of the registered seat of the Controller/Processor or its representative, if any, or in the court in whose district the data subject has his/her residence. The critical element for the establishment of the claim is the proof by the data subject of the causal link between his/her harm and the Incident.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

While there have been a few cases where administrative fines were imposed by the HDPA to companies for illegal processing of personal data (HELLENIC PETROLEUM GROUP) and for not taking adequate measures to safeguard the security of information systems that resulted in data breach (OLYMPION HOTEL, AEGEAN MARINE), there is not still any published case of a private action in relation to Incidents in the Greek jurisdiction on the basis of Regulation No. 2016/679/EC (GDPR) and the respective Greek Law 4624/2019. However, there are a number of civil dicta in relation to the unlawful processing of personal data on the basis of the previous personal data framework, namely Law 2472/1997, which is still in force in complementarity with Law 4624/2019.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

According to Art. 40 of Law 4624/2019, transposing Art. 79 GDPR into the Greek legal order, tort liability may be established for a Data Controller or a Data Processor in case a data subject suffers material or non-material damage from acts or omissions of the above persons violating the GDPR. More in particular, the negligence to prevent an Incident resulting in a data breach, falls within the scope of tort liability, giving rise to right of compensation of the affected data subject. Civil liability arising from torts – both material and moral – is regulated by the Greek Civil Code under Arts 914 and 932, respectively.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, it is permitted for organisations to take out cyber insurance against Incidents in Greece. Such an insurance package could indicatively include insurance coverage for cybercrime, reputational harm, dependent business interruption and telephone hacking.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration. The offered insurance package is formed after negotiation of the concerned party with the competent insurance agent, taking into account the provisions of the Greek Insurance Contract Act (2496/1997).

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The HDPA, the ADAE, the EETT, the Cyber Crime Unit of the Hellenic Police, as well as the HCA (established in 2018) are the competent authorities in Greece for the investigation of an Incident. According to Art. 148 of Law 4727/2020, the providers of public electronic communications networks or electronic communications services available to the public shall immediately notify the ADAE of any security incident that has had a significant impact on the operation of networks and services. The ADAE in turn: a) immediately notifies any event, of which it becomes aware in accordance with the previous paragraph, to the HCA; and b) notifies the events that have an impact on the availability or integrity of networks or services in the EETT. The ADAE also cooperates on a case-by-case basis, in accordance with the provisions of the current legislation, with the other competent law enforcement authorities, the HCA and the HDPA. Moreover, pursuant to Art. 149 of Law 4727/2020, the ADAE is assisted by the CSIRT.

It should be noted that the HCA, which reports to the Ministry of Digital Governance, consults and cooperates with the other competent national law enforcement authorities. The above-mentioned authorities, as law enforcement authorities, have the right to conduct audits and impose administrative fines or criminal sanctions in case they find that the existing institutional framework has been violated. In the public sector especially, the competent authority for dealing with/protecting against cyber-attacks and threats to the public body and the critical infrastructure of the country is the National Cyber Attack Authority – National CERT.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no provisions of national applicable laws that require organisations to implement backdoors in their IT systems for law enforcement authorities. Nevertheless, as part of inspections or audits, the competent authorities may inspect the technological infrastructure and other means, whether automated or not, by requesting access to all data and information required for the purposes of the relevant inspection and the performance of their duties, without the audited entity being able to oppose such due to any kind of secrecy.

Dr. Nikos Th. Nikolinakos is the Managing Partner of Nikolinakos & Partners LLP and co-head of the Competition Law, TMT and Digital Business practices. He features prominently in the Competition Law, TMT, Data Protection & Cybersecurity, and Intellectual Property rankings of leading Bar publications.

Nikos divides his specialised practice between regulatory and policy advice in the TMT sector, and in EU/national Competition Law, Data Protection & Cybersecurity, emerging digital technologies (such as AI and IoT), Intellectual Property rights advocacy and compliance. Prior to founding the firm, Nikos held the post of general counsel – legal and regulatory affairs director for a major telecoms operator and internet provider in Greece. He also held the position of senior in-house adviser to the EETT, responsible for Competition Law and Regulatory Policy/Compliance. He has filled senior consulting roles in various international projects for governments, national regulatory authorities, market players and the European Commission.

Nikos has been a Visiting Lecturer on Electronic Communications Law, Data Protection & Cybersecurity, Competition Law and Intellectual Property at the AIT Center and the National Technical University of Athens (NTUA). Nikos is the author of numerous contributions in books and refereed journals in the fields of TMT, New Technologies and Competition Law. He is also the author of EU Competition Law and Regulation in the Converging Telecommunications, Media & IT Sectors (2006, Kluwer Law International/Aspen Publishers).

Education: National and Kapodistrian University of Athens, School of Law (LL.B.); the University of Edinburgh, School of Law (LL.M. and Ph.D.).

Nikolinakos & Partners Law Firm
182, Mesogeion Avenue
P.C.15561, Athens
Greece

Tel: +30 2130 020 020
Email: nikolinakos@nllaw.gr
URL: www.nllaw.gr

Dina Th. Kouvelou is a Partner, head of the Data Protection & Cybersecurity practice and co-head of the Competition Law, TMT and Digital Business practices of Nikolinakos & Partners LLP. Dina is recommended as a leading TMT, Data Protection and Competition Legal Counsel by *The Legal 500* ("an outstanding regulatory counsel" who "provides a hard-to-find combination of technical and practical legal advice") and *Chambers and Partners* ("a true TMT expert", "a competition law expert who is extremely business oriented, proactive, and an effective strategist").

During the last 20 years, Dina's professional career has spanned TMT, Data protection & Cybersecurity, Betting and Gaming, Competition Law and Corporate/Commercial Law, with experience in, amongst others, the following roles: general counsel and head of legal & regulatory affairs in a leading alternative fixed telecoms operator and in a mobile operator in Greece; Senior Competition Law and Regulatory Policy Advisor in the Legal Department of the EETT; and Legal Consultant in Regulatory, Competition Law and Commercial Law projects with Greek and international law firms and consultancies.

Education: National and Kapodistrian University of Athens, School of Law; Queen Mary University of London (LL.M., Computer and Communications Law).

Nikolinakos & Partners Law Firm
182, Mesogeion Avenue
P.C.15561, Athens
Greece

Tel: +30 2130 020 020
Email: kouvelou@nllaw.gr
URL: www.nllaw.gr

Alexis N. Spyropoulos is a Partner, head of the Administrative Law & Public Procurement Practice of Nikolinakos & Partners LLP. He acted from 2007 to 2015 as Head of the Legal Department of the EETT, handling numerous complaints, actions, and infringement proceedings.

Alexis is experienced in representing undertakings and Government bodies in all kinds of proceedings (including Competition Law and Data Protection issues) before administrative courts and regulatory authorities. He has extensive (20 years) experience in the fields of TMT, Administrative Law, Data Protection & Competition Law.

Education: National and Kapodistrian University of Athens, School of Law; University of Sheffield, LL.M. in Commercial Law, Intellectual Property Law, Insurance Law & Competition Law.

Nikolinakos & Partners Law Firm
182, Mesogeion Avenue
P.C.15561, Athens
Greece

Tel: +30 2130 020 020
Email: spyropoulos@nllaw.gr
URL: www.nllaw.gr

India

Subramaniam & Associates (SNA)

Aditi Subramaniam

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Hacking is a criminal offence in India and may also lead to civil liabilities.

Section 43 of the Information Technology Act, 2000 (the "IT Act") proscribes, in respect of a computer, computer system, computer network or computer resource: unauthorised access; unauthorised downloads, copies or extraction of any data, information or computer database; introduction of "computer contaminants" or viruses; assistance of any person in order to facilitate access in contravention to the IT Act; and any manipulation or tampering that causes services availed by one person to be charged to another.

Prior to amendments to the IT Act in 2008, section 66 of said Act specifically defined hacking as the destruction, deletion or alteration of any information residing in a computer resource, or the diminishment of the value or utility of a computer resource, or an action that affects a computer resource injuriously. These actions are now within the purview of section 43 of the IT Act as amended in 2008, which no longer makes specific reference to the term "hacking" but otherwise retains the language of the former section 66. Finally, section 43 as amended also proscribes the stealing, concealment, destruction or alteration (or causing any person to do any of the foregoing) of any computer source code used for a computer resource with an intention to cause damage.

Those found guilty of offences under section 43 shall be punishable by imprisonment for a term of up to three years, a fine of INR 500,000, or both.

Denial-of-service attacks

Denial-of-service (DoS) attacks are also punishable under section 43 of the IT Act. Any person, who, without permission of the owner of a computer, computer system or computer network disrupts or causes disruption of said computer, computer system or computer network, and/or denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means, is punishable under sections 43(e) and (f). As indicated previously, contravention of the provisions of section 43 is punishable by imprisonment for a term of up to three years, a fine of INR 500,000, or both.

Phishing

The statute does not make explicit reference to phishing. However, in *National Association of Software and Services Companies v. Ajay Sood* 2005 (30) PTC 437 (Del), the Delhi High Court defined phishing as "…a form of internet fraud…" involving a deliberate misrepresentation or theft of identity in order to perpetrate theft of data. Section 43 of the IT Act broadly covers actions within this definition, which may be categorised as phishing attacks, as indicated in previous answers. Penalties for contravention of section 43 have also been specified above.

In addition, section 66C of the Information Technology (Amendment) Act, 2008 (the "IT Amendment Act") states that whoever fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of up to three years, and will also be liable to a fine of up to INR 100,000. Section 66D of the IT Amendment Act prescribes the same penalties for whoever, by means of any communication device or computer resource cheats by personation.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Section 43 of the IT Act makes it an offence for a person, without the permission of the owner of a computer, computer system, or computer network, to introduce or cause to be introduced any computer contaminant or computer virus into said computer, computer system or computer network.

The explanation to section 43 defines "computer contaminant" as "any set of computer instructions that are designed –

(a) To modify, destroy, record, transmit, data or programme residing within a computer, computer system or computer network; or

(b) By any means to usurp the normal operation of the computer, computer system or computer network".

The explanation defines "computer virus" as "any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource". Penalties for the contravention of section 43 are indicated above.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

The IT Act does not contain clauses directly referring to distribution, sale or offering for sale tools for use in the commission of cybercrime.

However, various provisions of section 43 penalise, in respect of a computer, computer system or computer network, a person

who: secures unauthorised access; causes computer contaminants and/or viruses to be introduced; causes damage; causes disruption; and/or causes the denial of access of any authorised persons. Additionally, section 43(g) proscribes the provision of any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the IT Act. Penalties for the contravention of section 43 are indicated above.

In addition, section 84B of the IT Amendment Act also proscribes the abetment of any offence under the IT Act or the IT Amendment Act. The statute states that if no express provision is made for the punishment of such abetment, the penalty thereon will be the punishment provided by the Act for the offence itself.

Possession or use of hardware, software or other tools used to commit cybercrime

The IT Act does not contain clauses directly referring to possession of tools for use in the commission of cybercrime. See the answer under the heading "Distribution, sale or offering for sale…" above.

Section 66B of the IT Amendment Act states that whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be a stolen computer resource or communication device shall be punished with imprisonment of up to three years, a fine of up to INR 100,000, or both.

Identity theft or identity fraud (e.g. in connection with access devices)

See the answer under the heading "Phishing" above.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

See the answer under the heading "Hacking" above.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

In addition to the offences discussed in the answer under the heading "Hacking" above, simply securing unauthorised access to a computer, computer system, computer network or computer resource is punishable under section 43. This is punishable as indicated in previous answers. However, the IT Act does not make specific reference to penetration testing.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Section 66F of the IT Amendment Act defines and penalises cyber terrorism. The provision states as follows:

"(1) Whoever –

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by—

(i) denying or cause the denial of access to any person authorised to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any computer contaminant,

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under Section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,

commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life."

1.2 Do any of the above-mentioned offences have extraterritorial application?

All provisions of the IT Act and IT Amendment Act apply to offences or contraventions outside the territories of India by any person, if such offence or contravention should involve a computer, computer system or computer network located in India.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

No, there are not.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

1. The IT Act and the Information Technology (Amendment) Act 2008

The IT Act contains provisions for the protection of electronic data. The IT Act penalises 'cyber contraventions' (Section 43(a)–(h)) and 'cyber offences' (Sections 63–74).

The IT Act was originally passed to provide a legal framework for e-commerce activity and sanctions for computer misuse, but now also addresses data protection and cybersecurity concerns.

2. The Information Technology Rules (the IT Rules)

The IT Rules focus on and regulate specific areas of the collection, transfer and processing of data, and include the following:

- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, which require entities holding users'

sensitive personal information to maintain certain specified security standards;

- The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, which prohibit content of a specific nature on the internet, and govern the role of intermediaries, including social media intermediaries, in keeping personal data of their users safe online;
- The Information Technology (Guidelines for Cyber Cafe) Rules, which require cybercafés to register with a registration agency and maintain a log of users' identities and their internet usage; and
- The Information Technology (Electronic Service Delivery) Rules, which allow the government to specify that certain services, such as applications, certificates and licences, be delivered electronically.

In addition to the legislation described above, enforcement may also sometimes occur on the basis of the Copyright Act, 1957. Depending on the circumstances, other legislation, such as the Indian Penal Code, 1860, the Code of Criminal Procedure, 1973, the Indian Telegraph Act, 1885, the Companies Act, 1956 and the Consumer Protection Act, 1986, may also sometimes apply.

In particular, the Indian Penal Code contains provisions covering most aspects of criminal laws, for instance, in respect of theft, fraud, identity theft and intentional causation of damage, which may, broadly speaking, apply to cyber offences. It is worth noting that the IT Act 2000 contains a *non-obstante* clause in section 81, stating that provisions of any other statute that may be inconsistent with those of the IT Act are overridden by the IT Act. However, the IT Amendment Act clarifies that this does not restrict any person from exercising any rights conferred under the Copyright Act, 1957, or the Patents Act, 1970.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

There are no industry- or sector-specific statutes making direct reference to cybersecurity requirements for operators of essential services or critical infrastructure. However, various national and industry bodies, some of which are established and empowered by statute, oversee cyber-hygiene and maintain industry standards.

The Data Security Council of India (DSCI) is a not-for-profit body established by the National Association of Software and Services Companies (NASSCOM), which develops and publishes best practices, standards and initiatives in cybersecurity.

The Reserve Bank of India (RBI) has issued a comprehensive Cyber Security Framework for all scheduled commercial banks (private, foreign and nationalised banks which are listed in the Reserve Bank of India Act, 1934). The framework requires all banks to adhere to strict cybersecurity and data protection guidelines. Generally speaking, the RBI sets the minimum standards and norms for banks and non-banking finance companies, and other lenders and payment services.

Similarly, the Indian Medical Council issues guidelines for the protection and security of health and medical data and ethical practices by physicians and medical services providers and oversees adherence thereto.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The IT Act requires all data processors, controllers and handlers to be bound by obligations of transparency, have a lawful basis for the processing of data and adhere to purpose limitation and data retention requirements. The legislation does not prescribe specific measures to be taken for monitoring, detection, prevention or mitigation of Incidents. However, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules state the following in section 8:

Reasonable Security Practices and Procedures –

(1) A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies.

(2) The international standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements" is one such standard referred to in sub-rule (1).

(3) Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule (1), shall get its codes of best practices duly approved and notified by the central government for effective implementation.

(4) The body corporate or a person on its behalf who have implemented either the IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through an independent auditor, duly approved by the central government. The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the body corporate or a person on its behalf undertakes significant upgradation of its process and computer resource.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and

Duties) Rules, 2013 (the CERT-In Rules) provide for the functioning of CERT-In (see the answer to question 2.6 below).

Rule 12 of the CERT-In Rules prescribes the operation of a 24-hour Incident Response Helpdesk. Any individual, organisation or corporate entity affected by cybersecurity Incidents may report the Incident to Cert-In.

The Annexure to the Rules identifies certain Incidents that shall be mandatorily reported to Cert-In as soon as possible. These are as follows:

- targeted scanning/probing of critical networks/systems;
- compromise of critical systems/information;
- unauthorised access of IT systems/data;
- defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites, etc.;
- malicious code attacks such as spreading viruses/worms/Trojans/botnets/spyware;
- attacks on servers such as databases, mail, and DNS, and network devices such as routers;
- identity theft, spoofing and phishing attacks;
- DoS and Distributed Denial of Service (DDoS) attacks;
- attacks on critical infrastructure, SCADA systems and wireless networks; and
- attacks on applications such as e-governance, e-commerce, etc.

Rule 12 also requires service providers, intermediaries, data centres and bodies corporate to report cybersecurity Incidents to CERT-In within a reasonable time in order to facilitate timely action. The Cert-In website provides methods and formats for reporting cybersecurity Incidents and provides information on vulnerability reporting and Incident response procedures.

Under rule 3(1)(l) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, all intermediaries shall also report cybersecurity Incidents and share related information with CERT-In in accordance with the CERT-In Rules.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The legislation mandates only reporting Incidents to the relevant authorities. There are no obligations to voluntarily report Incidents to affected individuals or third parties.

However, individuals/third parties have the ability to access information with regard to their own data at any time. Rule 5(6) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules mandates that the body corporate or any person on its behalf must permit data principals to review any information they may have provided to an organisation or body corporate that is processing said data.

The Personal Data Protection Bill 2019, which was tabled in Parliament as of December 2019 but has not yet passed into law, will broaden the scope of this right for data principals. The Bill provides the data principal with the option to obtain from the data fiduciary in a clear and concise manner, confirmation of whether its personal data is being (or has been) processed and a brief summary of processing activities. Arguably, when this information is solicited, the organisation in question is obligated to include any information with regard to an Incident if it directly affects the individual requesting this information. The Bill states that the data principal shall also have the right to access in one place the identities of the data fiduciaries with whom their personal data has been shared, along with the categories of such personal data.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

Under Section 70B of the IT Amendment Act, the Indian government has constituted the Indian Computer Emergency Response Team (CERT-In). CERT-In is a national nodal agency responding to computer security Incidents as and when they occur. The Ministry of Electronics and Information Technology specifies the functions of the agency as follows:

- collection, analysis and dissemination of information on cybersecurity Incidents;
- forecast and alerts of cybersecurity Incidents;
- emergency measures for handling cybersecurity Incidents;
- coordination of cybersecurity Incident response activities; and
- issuance of guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response to and reporting of cybersecurity Incidents.

The Ministry of Electronics and Information Technology established the Cyber Regulations Appellate Tribunal (CRAT) in October 2006 under section 48(1) of the IT Act. The IT Amendment Act renamed the tribunal the Cyber Appellate Tribunal (CAT). Pursuant to the IT Act, any person aggrieved by an order made by the Controller of Certifying Authorities or by an adjudicating officer under this Act may prefer an appeal before the CAT. The CAT is headed by a chairperson who is appointed by the central government by notification, as provided under Section 49 of the IT Act 2000. Before the IT Amendment Act, the chairperson was known as the presiding officer. Provisions have been made in the amended Act for CAT to comprise a chairperson and such a number of other members as the central government may notify or appoint.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Section 70B(7) of the IT Amendment Act states that any service provider, intermediaries, data centres, body corporate or person who fails to provide the information called for or to comply with the directions of CERT-In under section 70B(6) shall be punishable with imprisonment for up to one year or a fine of INR 100,000, or both. However, this provision applies only to non-compliance with specific requests for information by CERT-In under section 70B(6) of the IT Amendment Act.

Section 44(b) of the IT Act states that if a person who is required to furnish information under this Act or rules or regulations made thereunder fails to do so, he shall be liable to a penalty not exceeding INR 150,000 for each failure. This section also states that if a person who is required to furnish information fails to do so within a time period specified by the Authority, he shall be liable to a penalty not exceeding INR 5,000 for each day of delay until the failure continues.

Section 45 of the IT Act also provides for a residual penalty.

Whoever contravenes any rules or regulations under the IT Act, for the contravention of which no specific penalty has been provided, shall be liable to pay compensation not exceeding INR 25,000 to the affected party, or a penalty not exceeding INR 25,000.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The most recent examples of enforcement are sector-specific. For instance, in July 2021, the RBI recently imposed a monetary penalty of INR 50,000,000 on Axis Bank, which is one of India's largest private banks, for the contravention of provisions of its cybersecurity framework. Earlier that same month, the RBI had imposed a penalty of INR 2,500,000 on Punjab & Sindh Bank (a nationalised bank) for similar contraventions, after the bank reported a few cyber Incidents to the RBI in May.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
As indicated at question 2.3 above, all bodies corporate and other data fiduciaries are required to follow reasonable security practices and procedures to protect their systems. However, the legislation does not specifically refer to measures that may be taken to protect systems against Incidents.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
See the answer under the heading "Beacons" above.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
See the answer under the heading "Beacons" above.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

See the answers under question 3.1 above.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Not specifically. Indian laws do provide for export controls with respect to certain surveillance technologies. Additionally, under the Foreign Trade (Development and Regulation) Act No. 22 of 1992, the Directorate General of Foreign Trade (DGFT) defines items on the Indian Tariff Classification List and licenses the import and export of these items. The DGFT also maintains a separate list known as the Special Chemicals, Organisms, Materials, Equipment and Technologies (SCOMET) List, category 7 of which includes electronics, computers and information technology, including information security. However, category 7 does not explicitly define encryption software and/or hardware.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, it does. As there is no comprehensive cybersecurity legislation in India, practices vary based on sector- and industry-specific norms, the details of which are beyond the scope of this chapter. However, all entities must adhere to the provisions of the IT Act and various Rules promulgated under the Act, as well as the various other statutes specified in previous answers.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

The RBI prescribes rules and guidelines for entities within the financial services sector. The Insurance Regulatory and Development Authority prescribes similar rules for insurance companies. The Unified License Agreement requires all telecom companies to report Incidents to the Department of Telecommunications. Various other sector-specific rules exist, but a complete discussion of these rules is beyond the scope of this chapter.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

The IT Act and Rules do not explicitly address the issue of breach of directors' or officers' duties. However, section 85 of the IT Act does require that in the event of contravention of provisions of the Act, every person who was in charge of and was responsible to the company for the conduct of its business (including a director and any officer) at the time of the contravention shall be guilty of said contravention, shall be liable to be proceeded against, and shall be punished accordingly. The only exception to this is if said person or persons can prove that the contravention took place without their knowledge, or that they exercised due diligence to prevent it.

The Companies (Management and Administration) Rules, 2014, which were framed under the Companies Act, 2013, also require that the board of a company shall appoint a person in the company responsible for the management, maintenance and security of electronic records. Any failure by such person to do so would result in a breach of their duties of care under the law.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

There is no specific requirement for the designation of a Chief Information Security Officer. However, Rule 5(9) of the IT Rules mandates that all discrepancies or grievances reported to data controllers must be addressed in a timely manner. Corporate entities must designate grievance officers for this purpose, and the names and details of said officers must be published on the website of the body corporate. The grievance officer must redress respective grievances within a month from the date of receipt of said grievances.

The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 require the appointment of a Grievance Redressal Officer by all intermediaries, including social media intermediaries. The Rules also require that grievance redressal mechanisms be available to all users of social media intermediaries and be prominently published. Finally, the Rules prescribe specific timelines within which relevant action must be taken.

All remaining obligations for companies are described in sections 2 and 3 above.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

No, they are not.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Please see the answers in sections 1 and 2 above. No specific private remedies are available, but the IT Act and Rules make statutory remedies available to affected persons. Civil actions may be brought under section 43 of the IT Act, as discussed above.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

As at May 2021, no Indian companies have been penalised for data breaches since the drafting of the IT Act 2000. Cybersecurity Incidents have been reported to have impacted 52% of all organisations in India over this past year. Major Incidents include the compromise of passport details of 4.5 million passengers of Air India due to a data breach at the systems of airline data service provider SITA, and the order details of 180 million customers of Dominos Pizza. The COVID-19 test results of at least 1,500 Indian citizens also found their way online due to an attack on a government website.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

India has relatively young tort laws, and the incidence of litigation in this context is fairly low. However, in theory, persons affected by a cybersecurity Incident and suffering damages due to non-compliance of a body corporate with prevailing laws may have a negligence and/or professional negligence claim against said body corporate.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, they are. Cybersecurity insurance is not particularly common in this jurisdiction, but recent years have seen the concept pick up in popularity in certain sectors, including banking and information technology.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There is no general legislation on the subject. Regulatory limitations on coverage, if any, are sector-specific.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

In addition to the powers of CERT-In discussed in question 2.6 above, the agency may call for information from bodies corporate, data service providers, intermediaries and so on, as indicated in question 2.7. The IT Act also envisages a CAT in chapter X, which is not bound by the Indian Code of Civil Procedure, 1908 (CPC) and instead is at liberty to regulate its own procedures, limited only by the principles of natural justice and the IT Act itself. The CAT has the powers of a civil court under the CPC and, while trying a suit, such powers shall include:

- summoning and enforcing the attendance of any person and examining them under oath;
- requiring the discovery and production of documents or electronic records;
- requiring evidence on affidavits;
- issuing commissions for the examination of witnesses or documents;
- reviewing its decisions;
- dismissing an application for default or deciding it *ex parte*; and
- any other matter as may be prescribed.

In addition, section 80 of the IT Act provides the police with the discretion to enter a public place and search and arrest without a warrant any person found therein who is reasonably suspected of having committed, or of committing, or of being about to commit an offence under the IT Act.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Section 69 of the IT Act states that if the Controller of Certifying Authorities is satisfied that it is necessary or expedient to do so in the interests of: the sovereignty or integrity of India; the security of the State; friendly relations with foreign States; public order; or preventing incitement of the commission of any cognizable offence, for reasons to be recorded in writing, by order, any agency of the Government is to be directed to intercept any information transmitted through any computer resource. In such an event, the subscriber or person in charge of said computer resource shall, when called upon by the appropriate agency, extend all facilities and technical assistance to decrypt the information. The Act states that any failure to do so will result in imprisonment of up to seven years.

Aditi Subramaniam has a bachelor's degree in law from the University of Oxford and a master's degree in law from Columbia Law School. She is admitted to practise in India, has passed the New York Bar Examination and will be admitted to the New York Bar on 22 November 2021. Aditi brings to the firm expert legal drafting and research skills. She works primarily in patent and trade mark litigation and contentious matters before the IP tribunals and Appellate Board, and she routinely briefs senior lawyers for the same. She also advises clients on data protection and cybersecurity. As a litigator, in addition to intellectual property and allied matters, Aditi also handles contentious work in relation to real estate, taxation, labour and employment laws. She is a regular delegate at international IP conferences, and represents the firm at national and international seminars. In addition, she is a regular contributor to several international legal publications of repute.

Subramaniam & Associates (SNA)
M3M Cosmopolitan, 7th Floor
Golf Course Extension Road
Sector 66, Gurugram, 122001, Haryana
India

Tel: +91 124 4849700
Email: asm@sna-ip.com
URL: www.sna-ip.com

Subramaniam & Associates (SNA) is a full-service IP firm with 26 highly qualified attorneys. It boasts a very impressive list of clients and represents several Fortune 500 companies, leading corporations, universities and law firms from all over the world. It also represents a large number of domestic corporations worldwide. The firm is equipped to provide complete and highly cost-effective services, from drafting, filing and prosecution of applications to searches, oppositions and enforcement. It has an excellent network of associates and correspondent counsels worldwide. SNA is one of the largest filers of PCT International Applications from India and is regarded by the Indian Patent Office and the industry as a top IP firm in India.

SNA provides its clients with a personalised service – professional in approach and reliable irrespective of any time constraints. It possesses the latest technology and sophisticated software to enable its attorneys to keep track of all critical deadlines. The work systems are adapted to meet the specific needs of each client.

SNA's team of attorneys includes specialists in different technical fields as well as in litigation. SNA's clients are assured of easy access to appropriate advice at different stages in the creation, filing, prosecution, protection, management, exploitation and enforcement of their intellectual property.

With representation in major cities of India such as Calcutta, Chennai and Mumbai, and long-established relationships with local counsel throughout the world, SNA is well positioned to serve its clients' domestic and international needs.

www.sna-ip.com

SNA Subramaniam & Associates
Attorneys-at-Law • Patent and Trademark Agents

Ireland


Claire Morrissey


Kevin Harnett

Maples Group

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking is an offence under section 2 of the Criminal Justice (Offences Relating to Information Systems) Act 2017 (the "**2017 Act**"). A person who, without lawful authority or reasonable excuse, intentionally accesses an information system by infringing a security measure, commits an offence.

Denial-of-service attacks
Denial-of-service attacks are an offence under section 3 of the 2017 Act. A person who, without lawful authority: intentionally hinders or interrupts the functioning of an information system by inputting data on the system; transmits, damages, deletes, alters or suppresses, or causes the deterioration of, data on the system; or renders data on the system inaccessible, commits an offence.

Phishing
Phishing does not in itself constitute a specific offence in Ireland. However, it is possible that the activity would be caught by certain other, more general criminal legislation, depending on the circumstances (for instance, relating to identity theft or identity fraud). In this regard, see below.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infection of IT systems with malware is an offence under section 4 of the 2017 Act. A person who, without lawful authority, intentionally deletes, damages, alters or suppresses, or renders inaccessible, or causes the deterioration of data on an information system commits an offence.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Distribution, sale or offering for sale hardware, software or other tools used to commit cybercrime also constitutes an offence under the 2017 Act (section 6). It occurs when a person who, without lawful authority, intentionally produces, sells, procures for use, imports, distributes, or otherwise makes available, for the purpose of the commission of an offence under the 2017 Act, certain hacking tools.

Possession or use of hardware, software or other tools used to commit cybercrime
As above, possession or use of hardware, software or other tools used to commit cybercrime constitutes an offence under the 2017 Act (section 6).

Identity theft or identity fraud (e.g. in connection with access devices)
Although there is no precise, standalone offence of identity theft or identity fraud in this jurisdiction, it can nonetheless potentially be captured by the more general offence referred to as "making a gain or causing a loss by deception" (as contained in section 6 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (the "**2001 Act**")). This occurs where a person who dishonestly, with the intention of: making a gain for himself, herself or another; or causing loss to another, by any deception induces another to do or refrain from doing an act. In addition, sections 25, 26 and 27 of the 2001 Act cover specific forgery offences.

Separately, under section 8 of the 2017 Act, identity theft or fraud is an aggravating factor when it comes to sentencing, in relation to "denial-of-service attack" or "infection of IT systems" offences.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Electronic theft is covered by the relatively broad offence of "unlawful use of a computer", as provided for in section 9 of the 2001 Act. This occurs where a person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself, herself or another, or of causing loss to another.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Unsolicited penetration testing is an offence under the 2017 Act (section 2) where it involves intentionally accessing an IT system by infringing a security measure without lawful authority (i.e. permission of the system owner/right holder or where otherwise permitted by law) or "reasonable excuse". This term is not defined under the 2017 Act, and its application will depend on future judicial interpretation.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Section 5 of the 2017 Act creates the offence of "intercepting the transmission of data without lawful authority". This occurs when a person who, without lawful authority, intentionally intercepts any transmission (other than a public transmission) of data to, from or within an information system (including

any electromagnetic emission from such an information system carrying such data).

With regard to penalties, in relation to offences under the 2017 Act, the penalties range from maximum imprisonment of one year and a maximum fine of €5,000 for charges brought "summarily" (i.e. for less serious offences), to a maximum of five years' imprisonment (10 years in the case of denial-of-service attacks) and an unlimited fine for more serious offences. The relevant offences under the 2001 Act are only tried in the Circuit Court, with "making a gain or causing a loss by deception" carrying a maximum penalty of five years' imprisonment and an unlimited fine, and forgery and "unlawful use of a computer" offences carrying a maximum of 10 years and an unlimited fine.

1.2 Do any of the above-mentioned offences have extraterritorial application?

All of the above offences under the 2017 Act have certain extraterritorial application. Offenders may therefore be tried in Ireland, so long as they have not already been convicted or acquitted abroad in respect of the same act.

Although broader concepts such as, for instance, the "European arrest warrant" may be of relevance for Irish prosecutors, none of the above-mentioned offences under the 2001 Act carry, in and of themselves, extraterritorial application.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Each of the above offences under the 2017 Act contains the ingredient that it was committed without "lawful authority" (i.e. permission of the system owner/right holder or where otherwise permitted by law). Accordingly, prosecution of these offences will require, necessarily, that such authority or lawful permission was absent.

In addition, the offence relating to "hacking" carries a further qualification, i.e. where the person or company had a "reasonable excuse". This term is not defined under the 2017 Act, and so its application will depend on future judicial interpretation.

If a company is charged with any of the above 2017 Act offences where the offence was committed by an employee for the benefit of that company, it will be a defence for that company that it took "all reasonable steps and exercised all due diligence" to avoid the offence taking place.

It can be expected that judges will continue to take established factors into account when considering the appropriate penalty on foot of a conviction of a cyber-related crime (e.g. remorse, amends, cooperation with investigators, criminal history, and extent of damage).

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Apart from the above-referenced statutes in respect of criminal activity, Applicable Laws include the following:

- **Data Protection**: The General Data Protection Regulation (Regulation (EU) 2016/679) (the "**GDPR**") and the Data Protection Acts 1988 to 2018 (the "**DPA**") govern the manner in which personal data is collected and processed in Ireland. Data controllers are required to take "appropriate security measures" against unauthorised access, alteration, disclosure or destruction of data, in particular where the processing involves transmission of data over a network, and comply with strict reporting obligations in relation to Incidents. The DPA also provides for offences related to disclosure and/or sale of personal data obtained without prior authority.
- **e-Privacy**: The e-Privacy Regulations 2011 (S.I. 336 of 2011), which implemented the e-Privacy Directive 2002/58/EC (as amended by Directives 2006/24/EC and 2009/136/EC) (the "**e-Privacy Regulations**"), regulate the manner in which providers of publicly available telecommunications networks or services handle personal data and require providers to implement appropriate technical and organisational measures to safeguard the security of its services and report Incidents. It also prohibits interception or surveillance of communications and the related traffic data over a publicly available electronic communications service without users' consent. The draft EU e-Privacy Regulation is intended to replace the existing e-Privacy Directive and e-Privacy Regulations and expand the current regime to cover all businesses that provide online communication services.
- **Network and Information Systems**: The Security of Network and Information Systems Directive 2016/1148/EU (the "**NISD**") was transposed into Irish law under S.I. 360/2018 European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 (the "**NISD Regulations**"). The European Commission has adopted a proposal for a revised Directive on the Security of Network and Information Systems.
- **Payments Services**: The Payments Services Directive II (Directive 2015/2366/EU or "**PSD2**"), was transposed by the European Union (Payment Services) Regulations 2018 (S.I. 6 of 2018) (the "**Payment Services Regulations**"), and introduced regulatory technical standards (which were published by the European Banking Authority) to ensure "strong customer authentication" and payment service providers will be required to inform the national competent authority in the case of major operational or security Incidents. Providers must also notify customers if any Incident impacts the financial interests of its payment service users.
- **Other**: If there is a security breach that results in the dissemination of inaccurate information, persons about whom the inaccurate data relates may seek a remedy under the Defamation Act 2009 or at common law for breach of confidence or negligence.

See also sections 1 and 5.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The NISD Regulations and Commission Implementing Regulation (EU) 2018/151, which specifies further elements to be taken into account when identifying measures to ensure security of network and information systems, will apply. The

National Cyber Security Strategy 2019–2024 provides a mandate for the National Cyber Security Centre (the "**NCSC**") to engage in activities to protect critical information infrastructure. Enforcement powers under the NISD Regulations allow NCSC-authorised officers to conduct security assessments and audits, require the provision of information and issue binding instructions to remedy any deficiencies.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the GDPR and DPA, controllers are required to take appropriate measures, as outlined in questions 1.1 and 2.1 above. The GDPR and DPA do not detail specific security measures to be undertaken but, in determining appropriate measures, a controller may have regard to the state of technological development and the cost of implementing the measures. Controllers must ensure that the measures provide a level of security appropriate to the harm that might result from a breach and the nature of the data concerned. The Data Protection Commission (the "**DPC**") has issued guidance for controllers on data security, including recommending encryption, anti-virus software, firewalls, software patching, secure remote access, logs and audit trails, back-up systems and Incident response plans. At the outset of the COVID-19 pandemic, the DPC published guidance on protecting personal data when working remotely. It supplements existing DPC security guidance and focuses on keeping devices, emails, cloud and network access and paper records secure.

Under the e-Privacy Regulations, providers of publicly available telecommunications networks or services are required to take appropriate technical and organisational measures and ensure the level of security appropriate to the risk presented, having regard to the state of the art and cost of implementation. Such measures must ensure that personal data can only be accessed by authorised personnel for legally authorised purposes, protect personal data against accidental or unlawful destruction, loss, alteration, processing, etc., and ensure the implementation of a security policy.

The NISD Regulations require that operators of essential services ("**OES**") and digital services take appropriate measures to prevent and minimise the impact of Incidents affecting the security of the network and information systems used for the provision of essential and digital services with a view to ensuring continuity.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Where a personal data breach occurs, the controller shall, without undue delay and, where feasible, within 72 hours of becoming aware of the breach, notify the DPC of the breach. This notification shall include a description of the breach, the number or approximate number of data subjects concerned and personal data records concerned. It must also contain a list of likely consequences of the breach and measures taken or proposed to be taken to address the breach.

Where a data breach occurs that is likely to result in a high risk to the rights and freedoms of a data subject, the controller must notify the data subject to whom the breach relates. The requirement is waived where the controller has implemented appropriate measures to protect the data; in particular where the measures render the data unintelligible through encryption or otherwise to any person not authorised to access it. This notification must contain at least the same information provided to the DPC as described above. The DPC and European Data Protection Board have also published guidelines on data breach notification.

Providers of publicly available telecommunications networks or services are required to report information relating to Incidents or potential Incidents to the DPC (to the extent that such Incidents relate to personal data breaches). In the case of a particular risk of a breach to the security of a network, providers of publicly available telecommunications networks or services are required to inform their subscribers concerning such risk without delay and, where the risk lies outside the scope of the measures to be taken by the relevant service provider, any possible remedies including an indication of the likely costs involved. In case of a personal data breach, such providers must notify the DPC without delay and, where the said breach is likely to affect the personal data of a subscriber or individual, notify them also. If the provider can satisfy the DPC that the data would have been unintelligible to unauthorised persons, there may be no requirement to notify the individual or subscriber of the breach.

The NISD Regulations require OES and digital providers to notify the NCSC without delay of any Incident having a substantial impact on the provision of a service. The notification must provide sufficient information so that the NCSC can assess the significance of the same and any cross-border impact. The NISD Regulations stipulate that notification shall not make the notifying party subject to increased liability.

Section 19 of the Criminal Justice Act 2011 mandates reporting certain cybercrimes to the Irish police force, An Garda Síochána. Failure to make such a report, without reasonable excuse, is an offence.

The Central Bank of Ireland's (the "**CBI**") *Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks* (the "**Cross Industry Guidance**") requires firms to notify the Bank when they become aware of a cybersecurity Incident that could have a significant and adverse effect on the firm's ability to provide adequate services to its customers, its reputation or financial condition.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

See question 2.4 above.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

See question 2.4 above.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Failure to have appropriate security measures in place and/or report a data security breach in accordance with the GDPR can result in one of a number of administrative sanctions, including a ban on processing and fines up to €10 million or 2% of the global turnover (whichever is higher).

Failure by providers of publicly available telecommunications networks or services to comply with the above-mentioned requirements under the e-Privacy Regulations is an offence, liable to a fine of up to €250,000. If a person is convicted of an offence, the court may order any material or data that appears to it to be connected with the commission of the offence to be forfeited or destroyed and any relevant data to be erased.

Failure by an OES or a digital service provider to notify an Incident is an offence under the NISD Regulations liable to a fine of up to €500,000.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

2020 saw some high-profile enforcement activity in respect of these requirements. In July 2020, the CBI fined the Bank of Ireland €1.66 million in connection with a cyber fraud resulting in the transfer of client monies. In December 2020, the DPC fined Twitter €450,000 for failing to notify a personal data breach on time and adequately document the breach.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There is no specific prohibition on the use of beacons for such purposes, but careful consideration would need to be given as to whether such use might itself constitute "hacking" under the 2017 Act.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Subject to compliance with the various legislation identified above, there is no specific prohibition on the use of honeypots for such purposes.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Subject to compliance with the various legislation identified above, there is no specific prohibition on the use of sinkholes for such purposes.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Monitoring or interception of electronic communications on private networks to prevent or mitigate the impact of cyber-attacks must comply with the GDPR's requirements, including in relation to transparency, necessity and proportionality. The e-Privacy Regulations prohibit interception or surveillance of communications and the related traffic data over a publicly-available electronic communications service without users' consent.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

The export of dual-use technology (i.e. technology that can be used for both civil and military purposes) is restricted. Most dual-use items can move freely within the EU. However, a licence is required to export them to a third country (i.e. outside the EU). Very sensitive items, such as equipment or software designed or modified to perform "cryptanalytic functions", require a transfer licence for movement within the EU.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Traditionally market practice with respect to information security varied considerably in Ireland depending on the industry sector concerned. Businesses in industries recognised as being particularly vulnerable to Incidents, such as the financial services sector, were more likely to have adequate processes in place to effectively address cyber risk. With the onset of the COVID-19 pandemic, the increased reliance on remote working and technology accelerated investment in information security across all sectors. The pandemic also provided more opportunities for scams and cyber-attacks with the 2021 Conti cyber-attack on the Irish Health Service Executive (the "**HSE**") being the most high-profile. In response to the attack, the Garda Cybercrime Bureau, Ireland's cybercrime unit, seized domains used in the attack and is engaging with Europol and Interpol.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

(a) There is currently no specific legislation focused on cybersecurity applicable to organisations in the financial services sector, but the CBI's Cross Industry Guidance will apply. The publication makes a number of recommendations including (but not limited to): the preparation of a well-considered and documented strategy to address cyber risk; the implementation of security awareness training programmes;

the performance of cyber risk assessments on a regular basis; and the implementation of strong controls by firms over access to their IT systems. The NISD Regulations introduce security measures and Incident reporting obligations for credit institutions. See also reference to Payment Services Regulations in question 2.1 above. The European Commission's draft Digital Operational Resilience Act (the "**DORA**") published in September 2020 sees EU financial regulators expanding their focus beyond financial resilience to operational resilience including effective and prudent management of ICT risks and cybersecurity incidents. A Consultation Paper on the CBI's Cross Industry Guidance on Operational Resilience is currently active. The guidance will apply to all regulated financial service providers and includes recommendations regarding identifying, preparing for, responding to, adapting to and learning from operational disruptions, including cybersecurity incidents.

(b) As noted above, electronic communications companies (such as telecoms companies and ISPs) are governed by the GDPR, the DPA, and also the e-Privacy Regulations. Certain operators (IXPs, DNS service providers and TLD name registries) also now fall within the ambit of the NISD Regulations together with essential operators in the energy, transport, health, drinking water and digital infrastructure sectors.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

While there are no express directors' duties specific to cybersecurity, directors owe fiduciary duties to their company under common law and under the Companies Act 2014 (the "**CA 2014**").

There are a number of key fiduciary duties of directors set out in the CA 2014. This list, however, is not exhaustive. Some examples of directors' duties that could be considered to extend to cybersecurity are to:

- exercise the care, skill and diligence that would be exercised in the same circumstances by a reasonable person having both the knowledge and experience that may reasonably be expected of a person in the same position as the director, and the knowledge and experience that the director has;
- act honestly and responsibly in relation to the conduct of the affairs of the company;
- act in accordance with the company's constitution and exercise their powers only for the purposes allowed by law;
- exercise their powers in good faith in what the director considers to be the interests of the company; and
- have regard to the interests of their employees in general.

Directors have a general duty to identify, manage and mitigate risk, as well as fiduciary duties, such as those outlined above, which would extend to cybersecurity. Such duties are likely to be interpreted to mean that directors should have appropriate policies and strategies in place with respect to cyber risk and security and that directors should review and monitor these on a regular basis. Regard may also be had to compliance by a company with all relevant legislative obligations imposed on that company in assessing compliance by directors with their duties. Appropriate insurance coverage should also be considered.

Directors should be fully briefed and aware of all of the key issues relating to cyber risk. Larger organisations may choose to delegate more specific cyber risk issues to a specific risk sub-committee, but with the board retaining ultimate oversight and responsibility.

In relation to company secretaries, this will depend on what duties are delegated to the company secretary by the board of directors.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

While there are no such express obligations from a company law perspective, general directors' fiduciary duties, best corporate governance practices, as well as the "appropriate security" requirements under the DPA, may dictate that such actions are performed. See question 5.1 above for more detail on directors' duties. For industry-specific requirements, see question 4.1 above.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

While there are no such express obligations from a company law perspective, general director fiduciary duties, as well as best corporate governance practices, may dictate that such actions are performed. See question 5.1 above for more detail on directors' duties.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

As discussed in response to question 6.3 below, an Incident may give rise to various claims under the law of tort and under statute. It is also conceivable that an Incident would, depending on the circumstances, give rise to a claim for breach of contract.

In order to be entitled to compensation in damages, whether under a tortious or contractual analysis, a plaintiff will be required to establish: that a duty or obligation was owed to him/her by the defendant; that an Incident has occurred as a result of the defendant acting in breach of that duty or obligation; and loss or damage has been sustained to the plaintiff that would not have been sustained, but for the defendant's conduct.

Many classes of Incident may also give rise to claims for damages for breach of the constitutional right to privacy.

Where an Incident is committed by a State actor, for example, during the course of an investigation, it may give rise to an action in judicial review to prevent misuse of any inappropriately obtained data and/or to quash any decision taken in relation to, and/or on foot of, the Incident or any improperly obtained data (see, e.g. *CRH plc and Others v Competition and Consumer Protection Commission* [2017] IECS 34).

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

In the recent case of *Shawl Property Investments Limited v A & B*, decided in February 2021, the Court of Appeal considered the question of strict liability for data breaches, and, in allowing a claim for breach of data protection rights to progress to a plenary hearing, commented that: "*Nothing stated in s.117 or indeed the Act itself [the Data Protection Act 2018] suggests that a data protection action is a tort of strict liability.*"

In *Lannon v Minister for Social Protection,* a damages action by a man whose address was given by a then employee of the Department of Social Protection to a private detective hired by solicitors for a bank, was settled in the High Court in 2019. This followed a statement of acknowledgment and regret on behalf of the Department that "*data relating to Mr Lannon was released in contravention of the 1988 Data Protection Act by a former employee*".

There has also been significant speculation this year about the probability of the Conti cyber-attack on the HSE leading to large-scale civil actions against the Irish State.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Depending on the specific type of Incident concerned, liability for breach of statutory duty or in tort may arise. Examples of such liabilities are as follows:

- The DPA permits a data subject to take a data protection action against a controller or processor where they believe their rights have been infringed.
- A breach of a person's privacy rights may give rise to a claim in tort for breach of confidence or negligence, depending upon the circumstances.
- Incidents involving the theft of information or property may give rise to claims in the tort of conversion.
- Incidents involving the publication of intrusive personal information may, in some circumstances, constitute the tort of injurious or malicious falsehood.
- Incidents involving the misuse of private commercial information may give rise to claims for damages for tortious interference with economic relations.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Cyber insurance products are being taken up by businesses with increasing frequency and are now seen as routine. Such products afford cover for various data- and privacy-related issues including: the financial consequences of losing or misappropriating customer or employee data; the management of a data breach and attendant consequences, including the costs associated with involvement in an investigation by the DPC; and the costs associated with restoring, recollecting or recreating data after an Incident.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no specific regulatory limits placed on what an insurance policy can cover. However, GDPR and DPA administrative and criminal fines are not likely to be insurable in Ireland as a matter of public policy. Similarly, in the ordinary way, the consequences of intentional wrongdoing tend to be contractually excluded, as are the consequences of failure to remedy ascertained weaknesses or shortcomings in systems.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Under the 2017 Act, the Irish police force is given a relatively broad authority to investigate cybersecurity Incidents or suspected activity. Specifically, a warrant is obtainable so as to enter and search a premises, and examine and seize (demanding passwords, if necessary) anything believed to be evidence relating to an offence, or potential offence, under the 2017 Act, from a District Court Judge on foot of a suitable Garda statement, on oath.

The DPC has broad powers to investigate breaches under the DPA, including the power to enter business premises unannounced and without a court-ordered search warrant.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no requirements under Irish law for organisations to implement backdoors to their IT systems for law enforcement authorities, or to provide law enforcement authorities with encryption keys.

Claire Morrissey is a Partner and Head of the Dublin Data, Commercial and Technology practice at Maples and Calder, the Maples Group's law firm. Claire advises on a broad range of data protection issues and commercial contracts with a particular focus on compliance with the GDPR, technology and IP. In addition, Claire regularly advises on the technology, IP and data aspects of joint ventures and mergers & acquisitions.

Maples Group
75 St. Stephen's Green
Dublin 2, D02 PR50
Ireland

Tel: +353 1 619 2000
Email: claire.morrissey@maples.com
URL: www.maples.com

Kevin Harnett is a Partner in the Dublin Dispute Resolution & Insolvency team at Maples and Calder, the Maples Group's law firm. Kevin has extensive experience advising both domestic and multinational clients from diverse backgrounds on large and complex commercial disputes, including proceedings before the Commercial Court, as well as all forms of alternative dispute resolution. He has a particular focus on the financial services, technology, construction and property sectors.

Maples Group
75 St. Stephen's Green
Dublin 2, D02 PR50
Ireland

Tel: +353 1 619 2036
Email: kevin.harnett@maples.com
URL: www.maples.com

Japan


Hiromi Hayashi


Masaki Yukawa


Daisuke Tsuta

Mori Hamada & Matsumoto

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

As background, there are two main laws that criminalise cyber-attacks, namely (A) the Act on the Prohibition of Unauthorised Computer Access (the "**UCAL**"), and (B) the Penal Code.

(A) The UCAL imposes criminal sanctions on any person who makes an "**Unauthorised Access**" to a computer (an "**Access Controlled Computer**"), the access to and operation of which are under the control of an administrator (the "**Access Administrator**").

Unauthorised Access means any action that operates an Access Controlled Computer by either (i) inputting an identification code (*shikibetsu-fugou*) (e.g., password and ID) allocated to a user who is authorised to access the Access Controlled Computer (an "**Authorised User**"), without the permission of the Access Administrator or the Authorised User, or (ii) inputting any information (other than an identification code) or command that enables that person to evade control (e.g., cyberattack of a security flaw), without the permission of the Access Administrator (UCAL, Article 2, Paragraph 4).

The UCAL prohibits the following actions:

(a) Unauthorised Access (Article 3);

(b) obtaining the identification code of an Authorised User to make Unauthorised Access (Article 4);

(c) providing the identification code of an Authorised User to a third party other than the Access Administrator or the Authorised User (Article 5);

(d) keeping the identification code of an Authorised User that was obtained illegally to make Unauthorised Access (Article 6); and

(e) impersonating the Access Administrator or causing a false impression of being the Access Administrator by: (a) setting up a website where a fake Access Administrator requests an Authorised User to input his/her identification code; or (b) sending an email where a fake Access Administrator requests an Authorised User to input his/her identification code (Article 7).

Any person who commits (a) above (Article 3) is subject to imprisonment of up to three years or a fine of up to JPY 1,000,000 (Article 11). Any person who commits (b) to (e) above (Articles 4 to 7) is subject to imprisonment of up to one year or a fine of up to JPY 500,000 (Article 12). However, if the person committing (c) (Article 5) does not know that the recipient intends to use the identification code for Unauthorised Access, that person is subject to a fine of up to JPY 300,000 (Article 13).

(B) The Penal Code provides for criminal sanctions on the creation and provision of "**Improper Command Records**", which give improper commands, such as a computer virus, to a computer (*fusei shirei denji-teki kiroku*). Improper Command Records mean (i) electromagnetic records that give a computer an improper command that causes the computer to be operated against the operator's intentions or to fail to be operated in accordance with the operator's intentions, and (ii) electromagnetic or other records that describe such improper commands.

Under the Penal Code, any person who creates or provides, without any justifiable reason, Improper Command Records, or who knowingly infects or attempts to infect a computer with Improper Command Records, is subject to imprisonment of up to three years or a fine of up to JPY 500,000 (Article 168-2). Any person who obtains or keeps Improper Command Records for the purpose of implementing the foregoing acts is subject to imprisonment of up to two years or a fine of up to JPY 300,000 (Article 168-3).

In addition, the Penal Code provides for the following additional penalties:

(i) any person who obstructs the business of another by causing a computer used in that business to be operated against the operator's intentions, or to fail to be operated in accordance with the operator's intentions, by (a) damaging that computer or any electromagnetic record used by that computer, or (b) giving false information or an improper command to the computer, is subject to imprisonment of up to five years or a fine of up to JPY 1,000,000 (Article 234-2);

(ii) any person who gains or attempts to gain, or causes or attempts to cause a third party to gain, illegal financial

benefits by: (a) creating false electromagnetic records by giving false information or an improper command to a computer; or (b) providing false electromagnetic records for processing by a third party, in either case, in connection with a gain, a loss or a change regarding financial benefits, is subject to imprisonment of up to 10 years (Article 246-2); and

(iii) any person who creates, provides or attempts to provide electromagnetic records for the purpose of causing a third party to mistakenly administer matters that relate to rights, obligations or proofs of facts is subject to imprisonment of up to five years or a fine of up to JPY 500,000. However, if the act relates to records to be made by public authorities or public servants, the penalty is imprisonment of up to 10 years or a fine of up to JPY 1,000,000 (Article 161-2).

Hacking is Unauthorised Access under the UCAL, punishable by imprisonment of up to three years or a fine of up to JPY 1,000,000.

If the hacking is made through Improper Command Records, it is also punishable under the Penal Code (please see question 1.1, point 1, (B)). In addition, if a business is obstructed by such hacking, the crime is punishable by imprisonment of up to five years or a fine of up to JPY 1,000,000 (Penal Code, Article 234-2).

Denial-of-service attacks
These carry the same penalties as hacking.

Phishing
Article 7 of the UCAL prohibits phishing, while Article 4 of the UCAL prohibits obtaining any identification code through phishing. These actions are punishable by imprisonment of up to one year or a fine of up to JPY 500,000 (Article 12).

In addition, any person who gains illegal benefits by using identification codes obtained by phishing is subject to imprisonment of up to 10 years under Article 246-2 of the Penal Code.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
This carries the same penalties as hacking.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Other than the crime of providing Improper Command Records (see above) without any justifiable reason to any third party, which is subject to imprisonment of up to three years or a fine of up to JPY 500,000 (Penal Code, Article 168-2), there is no general prohibition against the distribution, sale or offering of hardware, software or other tools that may be used to commit a cybercrime.

Generally, if a person provides hardware, software or other tools knowing that those tools will be used for Unauthorised Access (see above) or to infect a computer with Improper Command Records, that person will be an accessory to these crimes. However, the Supreme Court has taken a relatively modest approach in punishing providers of software that can be used for either legitimate or illegal purposes. The Supreme Court on 19 December 2011 acquitted a developer of a P2P software that could be and actually was used for copyright violation, saying that a software provider may be punished as an accessory only if he knew that the software will be used for a specific criminal act or mostly for criminal acts. In this case, the court found that since the developer constantly warned users not to use the software in violation of any copyright, it was difficult to attribute knowledge to the developer.

Possession or use of hardware, software or other tools used to commit cybercrime
Any person who obtains or keeps Improper Command Records for the purpose of using such records is subject to imprisonment of up to two years or a fine of up to JPY 300,000 (Penal Code, Article 168-3).

As an example, nine people were prosecuted for uploading software that contained a computer virus to an online storage system, and that infected the computers of people who accessed the storage and downloaded the software from September to December 2016.

Identity theft or identity fraud (e.g. in connection with access devices)
This carries the same penalties as phishing.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
In addition to the criminal penalties applicable to phishing, electronic theft is penalised under the Unfair Competition Prevention Act. If a current or former employee: (a) acquires a trade secret of an employer through theft, fraud, threat or other illegal actions (the "**Illegal Actions**"), including Unauthorised Access; or (b) uses or discloses a trade secret of the employer acquired through Illegal Actions, for the purpose of obtaining wrongful benefits or damaging the owner of the trade secret, that employee is subject to imprisonment of up to 10 years or a fine of up to JPY 20,000,000, or both (Article 21, Paragraph 1). In addition, if that employee commits any of the foregoing acts outside Japan, the fine is increased to up to JPY 30,000,000 (Article 21, Paragraph 3).

Under the Copyright Act, any person who uploads electronic data of movies or music, without the permission of the copyright owner, to enable another person to download them, is subject to imprisonment of up to 10 years or a fine of up to JPY 10,000,000, or both (Article 119, Paragraph 1). Furthermore, any person who downloads electronic data that is protected by another person's copyright, and who knows of such protection, is subject to imprisonment of up to two years or a fine of up to JPY 2,000,000, or both (Article 119, Paragraph 3). In addition, any person who sells, lends, manufactures, imports, holds or uploads any device or program that may remove, disable or change technology intended to protect copyright (e.g., copy protection code) is subject to imprisonment of up to three years or a fine of up to JPY 3,000,000, or both (Article 120-2).

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Since there is no exemption for this type of testing, unsolicited penetration testing is punishable as Unauthorised Access.

Vulnerability testing without permission is generally not allowed. However, the National Institute of Information and Communications Technology (the "**NICT**") (and only the NICT) is allowed to conduct vulnerability testing without permission under the Law on the National Institute of Information and Communication Technology, which exempts the NICT from the prohibition against Unauthorised Access.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
This carries the same penalties as electronic theft.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The UCAL provides for the extraterritorial application of Articles 3, 4, 5 (except where the offender did not know the recipient's purpose) and 6 of the UCAL (Article 14).

The Penal Code also has extraterritorial application (Article 4-2).

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

The above-mentioned offences are not subject to exceptions such as "ethical hacking" or lack of intention to cause damage or make financial gains.

As discussed above (please see question 1.1), vulnerability testing without permission may be conducted only by the NICT based on a special law, and there are no general exceptions to similar activities for other persons.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

In addition to the UCAL, the Penal Code and the Unfair Competition Prevention Act described above, the following laws are also applicable to cybersecurity.

(A) Basic Act on Cybersecurity (the "BAC")

This provides the basic framework for the responsibilities and policies of the national and local governments to enhance cybersecurity. In July 2018, pursuant to the BAC, the Japanese government issued the Cybersecurity Strategy (drafted by the Cybersecurity Strategy Headquarters (the "**CSHQ**") and established under Article 25 of the BAC to promote Japan's cybersecurity measures, and its secretariat, the National Center of Incident Readiness and Strategy for Cybersecurity (the "**NISC**")). Since the Cybersecurity Strategy has been revised every three years, the NISC prepared and sought public comments on the draft of the Cybersecurity Strategy for the next period from 2021 to 2024, in July 2021.

Furthermore, the BAC obligates operators of critical infrastructure to make efforts to voluntarily and proactively enhance cybersecurity, and to cooperate with the national and local governments to promote measures to enhance cybersecurity. In December 2018, the BAC was amended to establish the cybersecurity council (the "**Cybersecurity Council**"). The Cybersecurity Council is intended to be the avenue to allow national and local governmental authorities and business operators to share information that may facilitate the proposal and implementation of cybersecurity measures. The Cybersecurity Council was established in April 2019 and has 265 participating entities as of June 2021.

(B) Telecommunication Business Act (the "TBA")

Article 4 of the TBA provides that (1) the secrecy of communications being handled by a telecommunications carrier shall not be violated, and (2) any person who is engaged in a telecommunications business shall not disclose secrets obtained while in office, with respect to communications being handled by the telecommunications carrier, even after he/she has left office.

The secrecy of communications protects not only the contents of communications but also any information that would enable someone to infer the meaning or the contents of communications. In this regard, data on access logs and IP addresses are protected under the secrecy of communications. If a telecommunications carrier intentionally obtains any information protected under the secrecy of communications, discloses protected information to third parties and uses protected information without the consent of the parties who communicated with each other, that telecommunications carrier is in breach of Article 4(1).

To prevent cyberattacks, it would be useful for telecommunications carriers to collect and use information regarding cyberattacks, e.g., access logs of infected devices, and share this information with other telecommunications carriers or public authorities. However, the TBA does not explicitly provide how a telecoms carrier may deal with cyberattacks without breaching Article 4(1). The Ministry of Internal Affairs and Communications (the "**MIC**"), the governmental agency primarily responsible for implementing the TBA, issued reports in 2014, 2015 and 2018 that addressed whether a telecoms carrier may deal with cyberattacks and the issues that may arise in connection with the secrecy of communications. The findings and contents of the MIC's three reports are included in the guidelines on cyberattacks and the secrecy of communications (the "**Guidelines**"), issued by the Council regarding the Stable Use of the Internet. This Council is composed of five associations that are the ICT Information Sharing and Analysis Center Japan (the "**ICT-ISAC Japan**"), the Telecommunications Carriers Association, the Telecom Services Association, the Japan Internet Providers Association, and the Japan Cable and Telecommunications Association. The Guidelines are not legally binding, although they carry a lot of weight because the MIC confirmed them before the Guidelines were issued.

Furthermore, in 2013, the MIC started a project called ACTIVE (Advanced Cyber Threats response InitiatiVE) that aims to protect internet users from cyberattacks by collaborating with ISPs and IT systems vendors. To prevent computer virus infections, ISPs that are members of ACTIVE may warn users or block communications in accordance with the Guidelines.

In addition, in May 2018, the TBA was amended to introduce a new mechanism that enables a telecommunications carrier to share with other carriers' information on transmission sources of cyberattacks through an association confirmed by the MIC as being eligible to assist telecommunications carriers. After the amendments became effective in November 2018, the MIC confirmed that the ICT-ISAC Japan to be that association in January 2019.

(C) Act on the Protection of Personal Information (the "APPI")

The APPI is the principal data protection legislation in Japan. It is the APPI's basic principle that the cautious handling of "**Personal Information**" under the principle of respect for individuals will promote the proper handling of Personal Information. Personal Information means information about specific living individuals that can identify them by name, date of birth or other descriptions contained in the information (including information that will allow easy reference to other information, which may enable individual identification) (Article 2, Paragraph 1). A business operator handling Personal Information may not disclose or provide Personal Information without obtaining the subject's consent, unless certain conditions are met.

To prevent cyberattacks, it would be useful for business operators to collect and use information regarding cyberattacks, e.g., access logs of infected devices, and share this information with other business operators or public authorities. However, if the information includes Personal Information, it would be subject to the restrictions on the use and disclosure of Personal Information under the APPI.

(D) the Japanese Foreign Exchange and Foreign Trade Act (the "FEFTA")

The FEFTA regulates the export of sensitive goods and technologies, including encryption software and hardware (please see question 3.3), as well as inward direct investments such as acquisition of shares in Japanese companies by non-Japanese investors. From the viewpoint of national security, prior notification to the Ministry of Finance and other competent authorities will be required for an acquisition of 1% or more of shares in a Japanese company that engages in information technologies, software, and telecommunications businesses, unless an exemption is applicable, and the foregoing authorities may order the cessation of the acquisition.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The UCAL requires Access Administrators to make efforts to manage the identification codes of Authorised Users, examine the validity of functions to control access to the Access Controlled Computer and implement necessary measures, including enhancing functions (e.g., encryption of codes, definite deletion of codes that have not been used for a long time, implementing a batch program to address a security flaw, program updates, and appointing an officer for network security) (Article 8).

The so-called "**Critical Information Infrastructure Operators**" are required to make efforts to deepen their interest and understanding of the importance of cybersecurity, and to voluntarily and proactively ensure cybersecurity for the purpose of providing services in a stable and appropriate manner (BAC, Article 6). Article 3(1) of the BAC defines Critical Information Infrastructure Operators as operators of businesses that provide an infrastructure that is a foundation of people's lives and economic activities that could be enormously impacted by the functional failure or deterioration of that infrastructure.

The CSHQ formulated the Cybersecurity Policy for Critical Infrastructure Protection as a non-mandatory guideline that designated 14 critical infrastructure areas under its coverage. These 14 areas are information and communication, financial services, aviation, airports, railways, electric power, gas supply, government and administrative supply, medical, water, logistics, chemical, credit card, and petroleum.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

(A) Cybersecurity Management Guidelines

The Ministry of Economy, Trade and Industry (the "**METI**") and the Independent Administrative Agency Information-technology Promotion Agency (the "**IPA**") jointly issued the Cybersecurity Management Guidelines (the latest version of which is as of November 2017). The guidelines describe three principles that the management of companies that have a dedicated division for information systems and that are utilising IT, should recognise to protect their company from cyberattacks, and 10 material items on which management should give instructions to executives or directors in charge of IT security, including the chief information security officer (the "**CISO**").

The 10 material items and some examples of recommended actions for each item described in the guidelines are as follows:

(i) Recognise cybersecurity risks and develop company-wide measures.
Example: Develop a security policy that incorporates cybersecurity risk management while aligning it with the company's management policy, so that management can publish company-wide measures.

(ii) Build a structure or process for cybersecurity risk management.
Example: The CISO establishes a system to manage cybersecurity risks and set forth the responsibilities clearly.
Example: Directors examine whether a system that will manage cybersecurity risks has been established and is being operated properly.

(iii) Secure resources (e.g., budget and manpower) to execute cybersecurity measures.
Example: Allocating resources to implement specific cybersecurity measures.

(iv) Understand possible cybersecurity risks and develop plans to deal with such risks.
Example: During a business strategy exercise, identify information that needs protection and cybersecurity risks against that information (e.g., damage from leakage of trade secrets on a strategic basis).

(v) Build a structure to deal with cybersecurity risks (i.e., structure to detect, analyse, and defend against cybersecurity risks).
Example: Secure the computing environment and network structure used for important operations by defending them through multiple layers.

(vi) Publish a cybersecurity measures framework (the "**PDCA**") and its action plan.
Example: Develop a structure or process where one can constantly respond to cybersecurity risks (assurance of implementation of a PDCA).

(vii) Develop an emergency response system (e.g., emergency contacts, initial action manual, and Computer Security Incident Response Team (the "**CSIRT**")) and execute regular hands-on drills.
Example: Issue instructions to promptly cooperate with relevant organisations and to investigate relevant logs to ensure that efficient actions or investigations can be taken to identify the cause and damage of a cyberattack.
Example: Execute drills, including planning activities, to prevent recurrence after Incidents and reporting Incidents to relevant authorities.

(viii) Develop a system to recover from the damages caused by an Incident.
Example: Establish protocols for recovery from business suspension, or other damages caused by an Incident, and execute drills in accordance with these protocols.

(ix) Ensure that entities in the company's entire supply chain, including business partners and outsourcing companies for system operations, take security measures.
Example: Conclude agreements or other documents to provide clearly how group companies, business partners, and outsourcing companies for system operations in the company's supply chain will take security measures.

Example: Have access to and understand reports on how group companies, business partners, and outsourcing companies for system operations in the company's supply chain take security measures.

(x) Collect information on cyberattacks through participation in information-sharing activities and develop an environment to utilise such information.
Example: Help society guard against cyberattacks by actively giving, sharing, and utilising relevant information.
Example: Report information on malware and illegal access to the IPA in accordance with public notification procedures (standards for countermeasures for computer viruses and for illegal access to a computer).

(B) Common Standards on Information Security Measures of Governmental Entities

The CSHQ and the NISC jointly issued the Common Standards on Information Security Measures of Governmental Entities under Article 26(1) of the BAC. The standards are a unified framework for improving the level of information security of governmental entities and define the baseline for information security measures to ensure a higher level of information security. Although these standards do not apply to private companies, some entities refer to these standards for their information security measures. The standards were amended in July 2021.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

There is no mandatory requirement to report Incidents.

However, under the guidelines for banks issued by the Financial Services Agency (the "**FSA**"), banks are required to report an Incident immediately after becoming aware of it. The guidelines are not legally binding; however, because the FSA is a powerful regulator of the financial sector, banks would typically comply with the FSA's guidelines (please see question 4.1). The report must include:

(i) the date and time when the Incident occurred and the location where the Incident occurred;
(ii) a summary of the Incident and which services were affected by the Incident;
(iii) causes of the Incident;
(iv) a summary of the facilities affected by the Incident;
(v) a summary of damages caused by the Incident, and how and when the situation was remedied or will be remedied;
(vi) any effect to other business providers;
(vii) how the banks responded to enquiries from users and how they notified users, public authorities, and the public; and
(viii) possible measures to prevent similar Incidents from happening.

In addition, if a cyberattack causes a serious Incident specified in the TBA and the enforcement rules of the TBA, such as a temporary suspension of telecommunications services or a violation of the secrecy of communications, the telecommunications carrier is required to report the Incident to the MIC promptly after its occurrence. In addition, the carrier is required to report the details of the said Incident to the MIC within 30 days from its occurrence. The detailed report must include:

(i) the date and time when the Incident occurred;
(ii) the date and time when the situation was remedied;
(iii) the location where the Incident occurred (the location of the facilities);
(iv) a summary of the Incident and which services were affected by the Incident;
(v) a summary of the facilities affected by the Incident;
(vi) details of the events or indications of the Incident, the number of users affected and the affected service area;
(vii) measures taken to deal with the Incident, including the persons who dealt with it, in chronological order;
(viii) causes that made the Incident serious, including how the facilities have been managed and maintained;
(ix) possible measures to prevent similar Incidents from happening;
(x) how the telecoms carrier responded to inquiries from users and how it notified users of the Incident;
(xi) internal rules in connection with the Incident;
(xii) if the telecoms carrier experienced similar Incidents in the past, a summary of the past Incidents;
(xiii) the name of the manager of the telecoms facilities; and
(xiv) the name and qualifications of the chief engineer of the telecoms facilities.

Furthermore, it is recommended that companies report the Incident to the IPA (please see question 2.3 above). The report must include:

(i) the location of where the infection was found;
(ii) the name of the computer virus. If the name is unknown, features of the virus found in the IT system;
(iii) the date when the infection was found;
(iv) the types of OS used and how the IT system is connected (e.g., LAN);
(v) how the infection was found;
(vi) possible cause of the infection (e.g., email or downloading files);
(vii) extent of the damage (e.g., the number of infected PCs); and
(viii) whether the infection has been completely removed.

The IPA also has a contact person whom the companies may consult, whether or not they file a report with the IPA, as to how they can deal with cyberattacks or any Unauthorised Access. According to the IPA's website, it had 9,698 consultations in 2020.

If the Incidents involve any disclosure, loss or damage of Personal Information handled by a business operator, then, according to the guidelines issued by the Personal Information Protection Committee (the "**PPC**") regarding the APPI, the operator is expected to promptly submit to the PPC a summary of such disclosure, loss, or damage (a "**Data Breach**") and planned measures to prevent future occurrences.

However, under the newest amendments to the APPI, which were promulgated on 12 June 2020 and will take effect in April 2022 (the "**Amended APPI**"), the business operator must report a Data Breach to the PPC in the following cases:

(i) a Data Breach of "Special Care-required Personal Information" (defined in the APPI), such as results of employees' health examinations;
(ii) a Data Breach of Personal Data (defined in the APPI) that poses a risk of financial damage to data subjects, such as credit card numbers;
(iii) a Data Breach caused by wrongful intent such as cyberattack or internal fraud;

(iv) a large number (more than 1,000 data subjects) of Data Breach occurrences; and
(v) when there is a possibility of any of the foregoing happening.

In addition, a business operator who undertakes "advanced encryption or other measures that are necessary to protect the rights and interests of the data subjects" will be exempted from the reporting or notification obligation, even if there is a Data Breach.

When a business operator recognises a Data Breach listed above or the possibility thereof, it must promptly submit a preliminary report on the matters known to it at the time, and must submit a definitive report within 30 days (60 days in the case of item (iii) above).

The report must include:
(i) an outline of the Data Breach;
(ii) details of personal data;
(iii) the number of Data Breach occurrences;
(iv) the cause of the Data Breach;
(v) the existence of secondary damage and details thereof;
(vi) the status of implementation of a response/notice to the data subjects;
(vii) the status of implementation of a public announcement;
(viii) measures to prevent recurrence; and
(ix) other matters that may be helpful for the PPC.

The PPC issued the amended guidelines in light of the 2020 APPI amendments (the "**amended PPC GL**") in August 2021.

According to the amended PPC GL, when a Data Breach or its possibility occurs, the business operator must take the following necessary measures, depending on the case:
(i) internal reporting and damage prevention;
(ii) investigation of the facts and the cause;
(iii) specifying the scope of impact; and
(iv) consideration and implementation of measures to prevent recurrence.

In addition, it is desirable to promptly disclose the relevant facts and measures to prevent recurrence, depending on the nature of the case.

The amended PPC GL interprets the phrase "possibility of Data Breach" as a case where the occurrence of a Data Breach is not known for certain but is suspected based on the facts known at the time.

Especially regarding cyberattacks, the following cases fall under the possibility of a Data Breach:
(i) traces of data theft due to Unauthorised Access are found;
(ii) confirmation of infection with malware that is known to behave in an information-stealing manner;
(iii) communication with the command and control server is confirmed; and
(iv) a business operator is informed by a security expert organisation that there is a possibility of a Data Breach based on certain grounds.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The Cybersecurity Management Guidelines recommend knowing who should be notified if a cyberattack has caused any damage, gathering information to be disclosed, and promptly publishing the Incident, taking into account its impact on stakeholders (please see question 2.3).

Furthermore, if the Incidents involve any disclosure, loss, or damage of Personal Information handled by a business operator, then, according to the guidelines issued by the PPC regarding the APPI, the operator is expected, depending on the contents or extent of the disclosure, loss or damage, to notify the affected individuals of the facts relevant to the disclosure, loss or damage, or to make the notification readily accessible to the affected individuals (e.g., posting the notification on the operator's website) in order to prevent secondary damages or similar Incidents.

However, under the Amended APPI, the business operator must notify the affected individuals of certain material Data Breaches (please see question 2.4).

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The MIC is the governmental agency primarily responsible for implementing the TBA.

The METI is not a regulator that has a specific mandated regulatory authority under specific laws. Rather, it promulgates desirable policies for each industry. The PPC is an independent organ that supervises the enforcement and application of the APPI.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Other than the report of a serious Incident under the TBA (please see question 2.4) and under the Amended APPI (please see questions 2.4 and 2.5), reporting is not mandatory. If a telecommunications carrier does not report a serious Incident, it is subject to a fine of up to JPY 300,000. If a business operator does not report a serious Incident under the Amended APPI, the PPC may make recommendations or issue orders, and if the operator does not comply with a PPC order, it is subject to imprisonment of up to one year or a fine of up to JPY 1,000,000.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

No examples can be found based on publicly available information.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

Applicable Laws do not differentiate between measures to detect and measures to deflect Incidents. Thus, the use of beacons is permissible so long as the use complies with the Guidelines and Applicable Laws.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Applicable Laws do not differentiate between measures to detect and measures to deflect Incidents. Thus, the use of honeypots is permissible so long as the use complies with the Guidelines and Applicable Laws.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Applicable Laws do not differentiate between measures to detect and measures to deflect Incidents. Thus, the use of sinkholes is permissible so long as the use complies with the Guidelines and Applicable Laws.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

As described in question 2.1, to prevent cyberattacks, the MIC issued reports that addressed whether a telecoms carrier may deal with cyberattacks and the issues that may arise in connection with the secrecy of communications, and the Council regarding the Stable Use of the Internet issued the Guidelines. These reports and the Guidelines cover policies regarding electronic communications on organisations' networks.

In addition, when a business operator monitors an employee's email or internet usage, monitoring may be considered illegal if the employees' Personal Information or privacy is not protected. The PPC recommends paying close attention to the following when conducting monitoring as part of employee supervision or personal data security management:

(a) identifying the purpose of monitoring, specifying the purpose in internal regulations, and informing the employees of the purpose;
(b) assigning a person responsible for monitoring and determining the authority of that person;
(c) establishing rules regarding the implementation of monitoring and ensuring that the organisation complies with them; and
(d) checking the adequacy of monitoring operations.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Under the FEFTA, encryption and intrusion program-related software and hardware are subject to export control regulations.

Regarding encryption, a cryptographic algorithm that meets certain requirements and any of the following three conditions is subject to export control regulations: (i) one main function is the security management of an information system; (ii) it constructs, manages, or operates a telecommunication line; and (iii) one main function is to record, store, and process information. However, there are many available exceptions. For example, hardware and software that use publicly known encryption technology or that secondarily use cryptographic functions are not subject to export control regulations.

Regarding intrusion program-related hardware or software (note that the intrusion program itself is not regulated), this cannot be exported if it includes vulnerability information and malware information about the program. However, in order to reduce the impact on cybersecurity practice, exporting such a hardware or software for the purpose of disclosing security vulnerabilities or responding to cyberattacks is exempt from export control regulations.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

In general, the financial business sector and the telecommunications service sector closely collaborate with relevant authorities on information security.

The FSA issued in 2015, and updated in 2018, a summary of its policies to strengthen cybersecurity in the financial business sector. According to the updated summary, the FSA will continue to: (i) promote continuous dialogue with financial institutions to understand their cybersecurity risks; (ii) improve information sharing among financial institutions; (iii) implement cybersecurity exercises in which financial institutions, the FSA, and other public authorities participate; and (iv) develop cybersecurity human resources and also respond to new issues such as accelerated digitalisation and international discussions. The FSA's guidelines require banks to, among others, establish an organisation to handle emergencies (e.g., the CSIRT), designate a manager in charge of cybersecurity, prepare multi-layered defences against cyberattacks, and implement a periodic assessment of cybersecurity. The guidelines are not legally binding; however, because the FSA is a powerful regulator of the financial sector, banks would typically comply with the FSA's guidelines.

As described above, telecommunications carriers are required to report a serious Incident specified in the TBA (please see question 2.5). In addition, if a telecommunications carrier does not take appropriate measures to remedy problems with its services, the MIC may order it to improve its business. Failure to comply with the order is subject to a fine of up to JPY 2,000,000.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Please see question 4.1.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Under the Companies Act, a director has the duty to act with "due care as a prudent manager" in performing his/her functions as director (*zenkan chuui gimu*). The applicable standard of care is that which a person in the same position and situation would reasonably be expected to observe. In general, if a director fails to get relevant information, enquire, or consider how to prevent Incidents, to the extent these acts are reasonably

expected of him/her based on the facts when he/she made a decision (e.g., decision to purchase the IT system), then he/she would be in breach of this duty.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

The Cybersecurity Management Guidelines, jointly issued by the METI and the IPA, recommend that companies build a structure or process for cybersecurity risk management and, as an example, designate a CISO according to the companies' policies, including the security policy (please see question 2.3).

Furthermore, the FSA's guidelines for banks provide the standards regarding cybersecurity management, such as establishing an organisation to handle emergencies (e.g., the CSIRT), designating a manager in charge of cybersecurity, and implementing a periodic assessment of cybersecurity (please see question 3.1).

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There are no disclosure requirements that are specific to cybersecurity risks or Incidents, but the NISC recommends in its "Framework of Cybersecurity in Corporate Management", published on 2 August 2016, that companies should disclose their initiatives and policies for cybersecurity in their information security report, CSR report, sustainability report, annual report, or corporate governance report. The survey commissioned by the NISC published in March 2019 showed that cybersecurity risk is referred to in annual reports of 74% of the 225 listed companies included in the Nikkei 225, which is an equity index of Japanese blue-chip companies.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Basically, if a person breaches a contract, the other party may bring a civil action based on the breach. The plaintiff has the burden of proving the breach, the damages incurred by it, and the causation between the breach and the plaintiff's damages.

In addition, the Civil Act of Japan provides for a claim based on tort. If a person causes damages to another, the injured party may bring a civil action based on tort. The plaintiff has the burden of proving the damages incurred by it, the act attributable to the defendant, and the causation between the defendant's act and the plaintiff's damages.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

A vendor of a computer system was sued by a company that used the system provided by the vendor. The case related to cyberattacks (SQL injections) to the system that resulted in the disclosure of credit card information of the company's clients. The company sought the payment of damages caused by the cyberattacks in the amount of approximately JPY 100,000,000, based on breach of contract. The Tokyo District Court decided that although the vendor was required to provide programs that are suitable for blocking SQL injections in accordance with existing standards when the computer system was provided, the Incident was also partially attributable to the company because it ignored the vendor's proposal to improve the system. The vendor was ordered to pay only approximately JPY 20,000,000 (Tokyo District Court decision dated 23 January 2014).

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Tort theory is available under the Civil Act of Japan (please see question 6.1).

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. In general, there are two categories of insurance against Incidents, namely (i) insurance to cover the losses incurred by the vendor of an IT system, and (ii) insurance to cover the losses incurred by a business operator using the IT system.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations on insurance coverage under the law. The coverage may differ depending on the insurance products of different insurance companies.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Law enforcers have the power to investigate Incidents that are related to crimes under Applicable Laws. Under the current police system, the prefectural police are responsible for investigations and the National Police Agency is responsible for policy making and analysis. The National Police Agency plans to establish a new bureau dedicated to cybercrimes and a new unit that will investigate serious Incidents independently or jointly with the prefectural police in 2022.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No, there are no such requirements.

Hiromi Hayashi is a partner at Mori Hamada & Matsumoto. Hiromi specialises in communications law and regulation and authored the Japanese section of The Preston Gates Guide to Telecommunications in Asia in 2005. Hiromi's other areas of practice are international and domestic transactions, takeover bids and corporate restructuring. Hiromi was admitted to the Bar in Japan in 2001 and in New York in 2007. Hiromi worked at Mizuho Corporate Bank from 1989–1994 and was with Davis Polk & Wardwell in New York from 2006–2007.

Mori Hamada & Matsumoto
16th Floor, Marunouchi Park Building
2-6-1 Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 5220 1811
Fax: +81 3 5220 1711
Email: hiromi.hayashi@mhm-global.com
URL: www.mhmjapan.com

Masaki Yukawa is counsel at Mori Hamada & Matsumoto. Masaki advises on cybersecurity issues for financial institutions, telecommunications businesses, and technology companies. Masaki was admitted to the Bar in Japan in 2009 and in California in 2016. Masaki worked at the Bank of Japan from 2003–2008 and was with the FSA from 2014–2015.

Mori Hamada & Matsumoto
16th Floor, Marunouchi Park Building
2-6-1 Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 6266 8764
Fax: +81 3 6266 8664
Email: masaki.yukawa@mhm-global.com
URL: www.mhmjapan.com

Daisuke Tsuta is an associate at Mori Hamada & Matsumoto. Daisuke specialises in cybersecurity and privacy laws. Daisuke was admitted to the Bar in Japan in 2010. Daisuke worked at the Kinki Local Finance Bureau of the Ministry of Finance from 2014–2015, at the MIC from 2015–2017, and at the NISC from 2017–2020.

Mori Hamada & Matsumoto
16th Floor, Marunouchi Park Building
2-6-1 Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 6266 8769
Fax: +81 3 6266 8669
Email: daisuke.tsuta@mhm-global.com
URL: www.mhmjapan.com

Mori Hamada & Matsumoto is a full-service international law firm based in Tokyo, with offices in other cities of Japan, and Bangkok, Beijing, Shanghai, Singapore, Yangon, and Ho Chi Minh. The firm has over 600 attorneys and a support staff of approximately 550, including legal assistants, translators and secretaries. The firm is one of the largest law firms in Japan and is particularly well known in the areas of mergers and acquisitions, finance, litigation, insolvency, telecommunications, broadcasting and intellectual property, as well as domestic litigation, bankruptcy, restructuring and multi-jurisdictional litigation and arbitration. The firm regularly advises on some of the largest and most prominent cross-border transactions representing both Japanese and foreign clients. In particular, the firm has extensive practice in, exposure to, and expertise on, telecommunications, broadcasting, the Internet, information technology and related areas, and provides legal advice and other legal services regarding the corporate, regulatory, financing and transactional requirements of clients in these areas.

www.mhmjapan.com

Kenya

Rilani Advocates

Nzilani Mweu

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Unauthorised access constitutes a crime under Section 14 of the Computer Misuse and Cybercrimes Act, 2018. The penalty for unauthorised access upon conviction is a fine not exceeding KES 5 million, imprisonment for a term not exceeding three years, or both.

Unauthorised access with the intent to commit or facilitate commission of a further offence is an offence and, upon conviction, results in a fine not exceeding KES 10 million, imprisonment for a term not exceeding 10 years, or both.

Denial-of-service attacks
Section 20 provides for enhanced penalties for offences of unauthorised access, access with intent to commit further offences, unauthorised interference and unauthorised interception involving protected computer systems. A protected computer system is defined as a system used in connection with: security and defence or international relations of Kenya; the provision of services directly related to communications infrastructure, banking and financial services, payment and settlement systems and instruments, and public utilities or transportation, including government services that are delivered electronically; and essential emergency services such as the police, civil defence and medical services, national registration systems and other related or similar services. The penalty is a fine not exceeding KES 25 million, imprisonment of up to 20 years, or both.

Phishing
Phishing is identified as an offence under Section 30 of the Computer Misuse and Cybercrimes Act and conviction results a penalty of KES 300,000 in fines, imprisonment for a maximum term of three years, or both.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
While the Act does not specifically define the offence of unauthorised interference to include the infection of IT systems with malware, the definition of the offence is broad enough to cover such infection of IT systems. The offence entails causing interference to a computer system, program or data intentionally and without authorisation, and it is immaterial whether the act is directed at a specific computer system program or data, a program or data of any kind, or a program or data held in any particular computer system. The penalty is a fine of not more than KES 10 million, imprisonment for not more than five years, or both.

Where the act leads to a person's significant loss, threatens security, causes physical injury or the death of a person, or threatens public health or safety, the penalty upon conviction is a fine of not more than KES 20 million, imprisonment for up to 10 years, or both.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Under Section 18(1), manufacturing, selling, adapting, importing, distribution or any other way of making available a device, password, access code or similar data, designed or adapted primarily for committing an offence under the Act, is an offence and, upon conviction, results in a fine not exceeding KES 20 million, imprisonment for a maximum term of 10 years, or both.

Possession or use of hardware, software or other tools used to commit cybercrime
Under Section 18(2), knowingly receiving or being in possession of a program or computer password, device, access code or similar data, designed or adapted primarily for committing an offence or assisting in the commission of an offence, constitutes an offence and, upon conviction, is liable to a fine of not more than KES 10 million.

Identity theft or identity fraud (e.g. in connection with access devices)
Under Section 29, identity theft or impersonation is an offence and, upon conviction, results in a fine of KES 200,000, two years' imprisonment, or both.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Under Section 16(3), unauthorised interference in a computer system program or data that results in significant financial loss to a person is an offence, resulting in a fine not exceeding KES 20 million, 10 years' imprisonment, or both.

Under Section 25, computer forgery that entails altering, deleting or suppressing computer data resulting in inauthentic data, with the intent that it be considered or acted upon for legal purposes as though it was authentic, regardless of whether that data is readable or intelligible, is an offence and results in a fine not exceeding KES 10 million, imprisonment not exceeding five years, or both. Where the offence is committed for wrongful gain, causing wrongful loss to another person or for any economic

gain for oneself or another person, the penalty is a fine of KES 20 million, imprisonment for not more than 10 years, or both.

Under Section 31, interception, destroying or aborting any messages through which money or information is being transferred is an offence resulting in a KES 200,000 fine, up to seven years' imprisonment, or both.

Under Section 41, employees are required to relinquish access codes and access rights to their employers immediately after the termination of their employment, and failure to do so is an offence, resulting in a fine of not more than KES 200,000, imprisonment for up to two years, or both.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

The Act does not expressly provide for penetration testing. However, where such testing is carried out without authorisation, it would amount to offences of unauthorised access, unauthorised interference and unauthorised interception.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Unauthorised disclosure of passwords, access codes or other means of gaining access to any program or data is an offence and, upon conviction, results in a fine not exceeding KES 5 million or imprisonment for a term not exceeding three years.

Fraudulent use of electronic data is an offence under Section 38 and entails knowingly and without authority causing any loss of property to another by altering, erasing, inputting or suppressing any data stored in a computer. The penalty is a fine of up to KES 200,000, imprisonment of up to two years, or both.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The Computer Misuse and Cybercrimes Act jurisdiction is limited to Kenya. However, there are certain circumstances where a crime committed outside Kenya falls within the scope of the Act. These are:

a) where the offence is committed outside Kenya by a citizen or resident of Kenya; and
b) where the offence is committed against a Kenyan citizen or property of the government of Kenya whether that property is in or outside Kenya.

In addition, the Act incorporates international co-operation implemented through the Mutual Legal Assistance Act and the Extradition (Contiguous and Foreign Countries) Act, where the office of the Attorney General may make a request to a foreign country for the investigation of an offence, and collection and preservation of evidence related to an act committed in contravention of the Act.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

The Computer Misuse and Cybercrimes Act does not provide for exemptions with regard to the offences. As the offences listed above are criminal in nature, the elements of intent, malice and premeditation are included in the framing of the offences.

The Act is silent on the committal of acts that are identified as offences, with no intent to cause damage, for financial gain, for research, testing systems or other purposes.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The Computer Misuse and Cybercrimes Act is the general law on cybercrime and cybersecurity. In Kenya, the Data Protection Act is also in effect, which covers aspects of cybersecurity.

There are also several sectoral laws, including the Kenya Information and Communications Act, which is applicable in the telecommunications sector) and under which the National Kenya Computer Incident Response Team Co-ordination Centre (National KE-CIRT/CC) is established) and is currently the national point of contact on cybersecurity, including monitoring, detection, prevention, mitigation and management of cybersecurity incidents. There is also the National Payment System Act, which is applicable in the financial sector and specifically for payment systems.

In addition, some other sectors like the health and banking sectors have guidelines and policies related to cybersecurity.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Under the Computer Misuse and Cybercrimes Act, there are specific requirements on the protection of critical infrastructure, which includes any vital systems, assets, facilities, networks or processes whose destruction would have debilitating effects on the availability, integrity or delivery of services essential to the health, safety, security and economic wellbeing of the Kenyan public or to the effective functioning of the government.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The Computer Misuse and Cybercrimes Act does not currently have any specific security obligations for organisations to monitor, detect, prevent or mitigate incidents. However, it is expected that these would be detailed in the regulations as well as the codes of practice and standards for operators of critical infrastructure and the framework for training on prevention, detection and mitigation of computer and cybercrimes that would be formulated by the National Computer and Cybercrimes Co-ordination Committee once constituted.

The National Computer and Cybercrimes Co-ordination Committee also has the mandate to, in consultation with critical infrastructure operators, recommend methods of securing systems, including the monitoring, detection, prevention and mitigation of incidents.

Under the Data Protection Act, data processors and data controllers are required to put in place technical and organisational measures for data security.

In the telecommunications sector, licensed entities are required, as part of their licensing requirements under the Kenya Information and Communications Act, to ensure the technical and organisational security of their systems and operations.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Under the Data Protection Act, organisations are required to report incidents of data breaches, including unauthorised access, where there is a real risk of harm to the data subjects. The report is to be made to the Office of the Data Protection Commissioner without delay and at the latest within 72 hours of becoming aware of that breach for data controllers. A data processor must inform the data controller of such incident within 48 hours. Where there is a delay, the report must explain: the delay in addition to including information on the nature of the breach; how and when it occurred; the number of data subjects affected; the classes of personal data affected by the breach; potential harm to the data subjects; a description of the measures the data controller or data processor intends to take or has taken to address the breach; recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise; where possible, the identity of the unauthorised person who may have accessed or acquired personal data; and the name and contact details of the Data Protection Officer or other contact point from whom more information may be obtained.

Under the Kenya Information and Communications Act, licensed telecommunications service providers are required to report any incidents interfering with their services to the Communications Authority and to the public within 24 hours, detailing the nature of the incident, the cause of the interruption and the steps being taken to rectify such interruption. However, the requirement is general and does not specifically include cybersecurity incidents.

In the financial sector, under the National Payment System Act and Banking Act, and specifically the Guidelines on Cybersecurity for the banking sector and payment service providers respectively, licensed banks, payment system service providers and other licensed entities are required to maintain records of any material service interruptions, major security breaches interfering with their services, incidents of fraud and any other concerns to the Central Bank of Kenya. They are further specifically required to report to the Central Bank, within 24 hours, any cybersecurity incidents that could have a significant and adverse effect on the ability to provide adequate services to customers and detail the reputational and financial impact of the incident.

Under the Computer Misuse and Cybercrimes Act, any person who operates a computer system or network, whether private or public, has an obligation to immediately report to the National Computer and Cybercrimes Co-ordination Committee created under the Act, any attacks, intrusions, and other disruptions to the functioning of another computer system within 24 hours of such attack, intrusion, or disruption. The report must detail the nature of the breach, how it occurred, an estimate of the number of people affected by the breach, an assessment of the risk of harm to the affected people, and an explanation of any circumstances that would delay or prevent the affected persons from being informed of the breach. Failure to report is an offence and, upon conviction, a person would be liable to a fine of up to KES 200,000, imprisonment for up to two years, or both.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Under the Data Protection Act, a data controller or processor is required to inform the data subject of any breach affecting their personal data within a reasonable time, unless the identity of the data subject cannot be established. However, the data controller may delay informing the data subject or restrict information provided if appropriate for prevention, detection or investigation of an offence, and may opt to not disclose the incident at all if the data controller or data processor has implemented the appropriate security safeguards, which may include encryption of affected personal data.

Under the Kenya Information and Communications Act, service providers are required to notify the public and their consumers of the interruption in services, the nature of the interruption and expected downtime period. However, the nature of the incidents or service interruptions is not defined to expressly state that cybersecurity incidents are included.

Financial services providers and payment system providers are required to notify their customers and other affected individuals of any interruption to their services.

The Computer Misuse and Cybercrimes Act does not expressly provide for notification to persons affected by a cybersecurity incident.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The Office of the Data Protection Commissioner is responsible for general implementation of the Data Protection Act.

In the telecommunications sector, the regulator is the Communications Authority of Kenya, while the regulator in the financial sector is the Central Bank of Kenya.

The National Computer and Cybercrimes Co-ordination Committee was created under the Computer Misuse and Cybercrimes Act, in order to co-ordinate matters relating to cybercrime and cybersecurity, but is yet to be constituted.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Under the Data Protection Act, failure by a data controller or processor to comply with its obligations under the Act, including

reporting of incidences of breach, may result in administrative fines of up to KES 5 million or 1% of an undertaking's annual turnover for the preceding year – whichever is lower – imposed by the Data Commissioner.

Under the Kenya Information and Communications Act, failure to report an incident or comply with other licensing terms leads to the imposition of administrative fines of up to 0.2% of the annual gross turnover for the preceding year.

Failure to provide information to the Central Bank of Kenya under the National Payment System Act is an offence resulting in a fine of not more than KES 500,000, one year's imprisonment, or both.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Both the Data Protection Act and the Computer Misuse and Cybercrimes Act, which provide general requirements on reporting of cybersecurity incidents, are relatively new and are not fully implemented. Currently, there are no reported incidents of non-compliance under the two Acts.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

There are no express requirements for organisations to use beacons to protect their IT systems. As organisations are encouraged to put in place adequate security measures and the determination of what is adequate is generally left to their discretion, the use of beacons where appropriate would be acceptable.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

There are no express requirements for organisations to use honeypots for their security measures and they are at liberty to implement any security measures they deem necessary and appropriate.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)

There is no specific requirement to use sinkholes for security measures by organisations. However, as organisations are encouraged to put in place adequate security measures, sinkholes may be utilised.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

While there is no express requirements for organisations to monitor and intercept electronic communication as part of mitigating incidents under the Computer Misuse and Cybercrimes Act, organisations are encouraged to determine the actions necessary for the prevention or mitigation of cyber-attacks. In addition, once an incident is reported and there is an ongoing investigation into an offence or suspected offence, the officer investigating may apply for a court order to compel a service provider to, within its existing technical capabilities, intercept the necessary content data and facilitate real time collection of such data.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

There are no restrictions under Kenyan law on importation or exportation of technology designed to prevent or mitigate the impact of cyber-attacks. Organisations are encouraged to put in place the best possible solutions they can obtain or access.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Generally, organisations in regulated sectors have a specific standard to meet with regard to the level of information security they implement. In addition, organisations in high-business segments, such as money transfer and mobile telecommunications, implement the highest levels of security for their systems.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

In the financial sector, the regulator issues guidelines on management of cybersecurity and has so far issued Guidelines on Cybersecurity for banks and payment service providers.

In telecommunications, licensed providers are required to ensure the security of their systems and protection of the data they collect and process.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Generally, the Board of Directors is required to make decisions on the running of the company and ensure any risks the company may face are mitigated. While specific obligations set out in law are dependent on the sector, such the financial sector, where the board is shown to have acted negligently, or knew about but did not take any action to prevent an incident, the board may be held liable for the commission of an offence by the company under the Computer Misuse and Cybercrimes Act

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

The requirements on the governance and appointment of Chief Information Security Officer (CISO) or equivalent are sector-based. For example, in the financial sector, banking institutions and payment service providers are required to appoint a CISO. They are also required to maintain records of incidents and to report cybersecurity incidents in a specified written format. The institutions are also required under the Guidelines on Cybersecurity and Prudential Guidelines to carry out assessments and testing periodically and to ensure their third-party vendors comply with legal and regulatory frameworks as well as international best practices.

While under the Capital Markets Authority (Corporate Governance) Regulations 2011 there is no requirement for appointment of a CISO, the board is tasked with the appointment of officers and employees to ensure the smooth running of the organisation.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There are currently no other specific disclosure requirements.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

As the offences under the Computer Misuse and Cybercrimes Act are criminal in nature, the elements of intent and commission of the criminal act would need to be met. The causation of injury of harm is not necessary in some of the offences. The Act provides to compensation orders where if a person is convicted of an offence, the court may further order for the payment of an amount to be fixed by the court as compensation by that person to the person harmed. This does not prejudice the right to pursue civil recovery of damages beyond the amount of compensation.

Where there is actual harm, loss or damage caused, the victim of the offence is at liberty to institute civil proceedings provided they can prove liability on a balance of probabilities.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

As the Computer Misuse and Cybercrimes Act is not fully implemented, there are currently no published actions relating to the offences under the Act.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Where an offence is committed by an organisation, any principal officer of that organisation is considered to have committed the offence unless they can prove that the offence was committed without their knowledge or consent and that they exercised diligence to prevent the commission of the offence.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

The Computer Misuse and Cybercrimes Act does not expressly provide for whether or not organisations can take out insurance against cybersecurity incidents. Sectoral laws are also silent on the same. However, with the risks of loss and damages posed by cybercrime, many organisations make a business decision to take out insurance against possible incidents.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

As the law does not expressly address insurance against cybersecurity incidents, the products related to such insurance are at the discretion of insurance providers.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Offences under the Act are subject to the investigatory powers of the National Police Service without prejudice to powers granted under the National Police Service Act, National Intelligence Services and the Kenya Defence Forces Act as necessary. Law enforcement officers have powers to:

a) search and seizure of stored computer data subject to obtaining a search warrant;
b) obtain a production order for specific computer data from a competent court;
c) through a court order, require expedited preservation for a period of 30 days, or as may be extended by the court, and partial disclosure of traffic data stored in a computer system that is reasonably required for an investigation, and there is risk the traffic data may be lost, modified or rendered inaccessible;
d) through a court order, require real time collection of traffic data associated with specified communication related to the person under investigation; and
e) through a court order, require the interception of content data and to compel a service provider to collect or record content data and to co-operate in collection and recording of content data in real time of specified communications.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are currently no legal requirements for organisations to implement backdoors in their IT systems for law enforcement authorities, or to provide law enforcement authorities with encryption keys.

Nzilani Mweu is the founder of Rilani Advocates, based in Nairobi, Kenya and has over 10 years of policy, regulatory, and transactional experience in the telecommunications, digital financial services, technology, competition, data protection, cybersecurity, intellectual property and commercial sectors.

She has advised regional and global corporations on privacy and data protection, with information privacy and security requirements and compliance with international best practices on data protection laws and policies and has experience in cybercrime and cybersecurity law. She has also been actively involved in shaping policy on the right to privacy and the collection of personal data under the recent amendments to the Registration of Persons Act in Kenya.

Nzilani is currently advising several multinational clients on various sectors, including digital financial services, digital banking, structuring businesses, technology, telecommunications, and manufacturing.

Nzilani was admitted to the Kenyan Bar in 2011 and holds a Bachelor of Laws (LL.B.) from Moi University and a Post-Graduate Diploma from Kenya School of Law. She also holds a Certificate in Law for Economic Regulation and Competition awarded by the University of Nairobi.

Nzilani is a member of the East African Law Society and the Law Society of Kenya and has previously served as a Member of the Intellectual Property and Information Communications and Technology Law Committee of the Law Society of Kenya. She is a member of the Lawyers in Technology Circle whose membership comprises leading women lawyers in Technology in Kenya.

Nzilani is a member of International Advisory Experts as the Kenyan expert on Intellectual Property, Technology and Telecommunications Law. She is also a member of the International Association of Privacy Professionals (IAPP) and is currently training to undertake the Certified Information Privacy Manager (CIPM) certification.

Rilani Advocates
D5 Riara Centre, Riara Road
P.O. Box 25518-00100
Nairobi
Kenya

Tel: +254 20 242 5260
Email: nzilani@rilaniadvocates.legal
URL: https://rilaniadvocates.legal

Rilani Advocates is a commercial law firm based in Nairobi, Kenya offering bespoke legal solutions. Our Advocates have experience dealing with complex issues across different sectors.

With our cross-cutting expertise, we provide seamless services while maintaining efficiency and accessibility. At Rilani Advocates, your business is our business. We seek to understand our client's business strategies, aspirations and set-up so that we can provide solutions tailored to their specific needs and offer precise legal strategy. We aim to build relationships for and with our clients to ensure they succeed.

Innovation is at the centre of how we operate, and we seek to provide cutting-edge legal solutions to support today's fast-paced technology-driven business environment and complex challenges. We adopt innovative solutions that redefine the role of lawyers in the success of businesses in today's fast-paced market and leverage technology to stay efficient. We aim to build long-term, personalised relationships with our clients based on the highest standards of professionalism, reciprocity, trust, and ethics. Our expertise in emerging business models and technology helps us understand your business needs and deliver exceptional results. Our success is measured by your satisfaction, growth, and success.

With our regional and international networks, we support our clients' businesses across borders.

https://rilaniadvocates.legal

Mexico

Creel, García-Cuéllar, Aiza y Enríquez

Begoña Cancino Garín (Former Partner)

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
The Federal Criminal Code provides for two different criminal types when it comes to unauthorised access: simple; and aggravated. The aggravation criteria depend on the purported intention to cause damages by obtaining a specific result with the unauthorised access, especially when it entails the violation of intellectual property rights. Unauthorised access is then a federal crime under articles 211 *bis* 1 to 211 *bis* 7 of the Federal Criminal Code, but also article 426, which is contained in a chapter devoted exclusively to copyrights and provides that performing any act with the purpose of breaking an encrypted satellite signal or carrying programs without the proper authorisation would be penalised with imprisonment from six months to four years, as well as a fine. Development and distribution of equipment intended to receive an encrypted signal, and services intended to receive or assisting others in receiving an encrypted signal, will be also penalised as described in this paragraph.

Also, the Federal Criminal Code provides that a person who, with or without authorisation, modifies, destroys or causes loss of information contained in credit institutions' systems or computer equipment protected by a security mechanism shall be penalised with imprisonment of up to six months to four years, as well as a fine. Moreover, an unauthorised person who knows or copies information from credit institutions' computer systems or equipment protected by a security mechanism shall be subject to imprisonment of three months to two years, as well as a fine.

Denial-of-service attacks
The Federal Criminal Code does not provide any definition, or similar definition, for this criminal offence. However, article 427 *quater* includes penalties of imprisonment from six months to six years and a fine to those who provide services to the public aimed primarily at circumventing an effective technological protection measure of any work of authorship (including, of course, software).

Phishing
The Federal Criminal Code does not provide any definition for phishing; however, such criminal offence could be considered fraud. According to article 386 of the Federal Criminal Code, a person commits fraud when he/she handles information through deceit, takes advantage of errors or misleads a person with the intent of obtaining a financial gain. In such case, the responsible party shall be subject to imprisonment of three days to 12 years, as well as a fine.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
The Federal Criminal Code does not provide any definition for this criminal offence; however, this type of behaviour may fall under the scope of hacking. The aforementioned penalties are applicable in this case. If the criminal offence is committed against the state, the relevant authority shall be subject to imprisonment of one year to four years, as well as a fine.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
The Federal Criminal Code does not provide any definition for phishing; however, such criminal offence could be considered fraud. According to article 386 of the Federal Criminal Code, a person commits fraud when he/she handles information through deceit, takes advantage of errors or misleads a person with the intent of obtaining a financial gain. In such case, the responsible party shall be subject to imprisonment of three days to 12 years, as well as a fine.

Possession or use of hardware, software or other tools used to commit cybercrime
The Federal Criminal Code provides that those who, knowingly, without authorisation and for profit, suppress or alter, by themselves or through another, any information on rights management, will be imposed with six months' to six years imprisonment and a fine. The same penalty will be imposed on any person who, for profit: distributes, or imports for distribution, information on rights management, knowing that it has been suppressed or altered without authorisation; or distributes, imports for distribution, transmits, communicates or makes available to the public, copies of works, performances, performances or phonograms, knowing that the information on rights management has been suppressed or altered without authorisation.

Identity theft or identity fraud (e.g. in connection with access devices)
The Credit Institutions Law provides that a person who produces: manufactures; reproduces; copies; prints; sells; trades; or alters any credit card, debit card or, in general, any other payment instrument, including electronic devices, issued by credit institutions, and without authorisation of the holder, shall be given a prison sentence of three to nine years, by the relevant authority, as well as a fine.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
As mentioned, identity theft and identity fraud are penalised under the Credit Institutions Law. If such activities are committed by any counsellor, official, employee or service provider of any credit institution, there would be grounds for alleging breach of confidence and the penalties would increase.

In addition, under the Mexican Industrial Property Law, the theft of trade secrets – by electronic means or not – by current or former employees constitutes a crime and triggers imprisonment and fines to the responsible parties.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
The Federal Criminal Code does not provide any definition for this criminal offence; however, this type of behaviour may fall under the scope of hacking. The aforementioned penalties are applicable in this case. If the criminal offence is committed against the state, the relevant authority shall impose a prison sentence of one year to four years, as well as a fine.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
In addition, activities such as espionage, conspiracy, crimes against means of communication, tapping of communications, acts of corruption, extortion and money laundering could be considered threats to the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data.

The Federal Criminal Code includes a complete chapter devoted to crimes in connection with copyrights, where the unauthorised production, reproduction, introduction in the country, storage, transportation, distribution, commercialisation or other uses for commercial speculation purposes will be sanctioned with imprisonment and fines.

1.2 Do any of the above-mentioned offences have extraterritorial application?

In principle, all of the above-mentioned offences are applicable only within Mexican territory; however, there might be cases of serious criminal offences in which the Mexican authorities may collaborate with other authorities in other jurisdictions.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

The Federal Criminal Code does not provide for any exception such as "ethical hacking"; however, it should be noted that most of the crimes referred therein will be considered as such if the activity has been carried out for profit or with the aim to cause damage.

The Federal Law against Organized Crime provides that in the investigation of a crime where it is assumed on good grounds that a member of organised crime is involved, it is possible to tap private communications by means of electronic systems and subject to a judicial order. The same occurs with the General Law to Prevent and Sanction Kidnapping Crimes, and when the Mexican government must request a judicial warrant to intercept private communications for national security purposes. Accordingly, the Federal Telecommunications and Broadcasting Law ("FTBL"), in its articles 189 and 190, allows competent authorities to control and tap private communications and provide support to those official requests.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Please see the following Applicable Laws:

- the Mexican Constitution;
- the FTBL;
- the Federal Law on the Protection of Personal Data held by Private Parties (the "Data Protection Law"), its regulations, recommendations, guidelines and similar regulations on data protection;
- the Federal Law on Transparency and Access to Public Information;
- the General Law on Transparency and Access to Public Information;
- General Standards as specified under the Mexican Official Standard regarding the requirements that shall be observed when keeping data messages;
- the Law on Negotiable Instruments and Credit Operations;
- the Mexican Federal Tax Code;
- the Credit Institutions Law;
- the Sole Circular for Banks;
- the Industrial Property Law;
- the Mexican Copyright Law;
- the Federal Labour Law;
- the Federal Criminal Code;
- the Law of the National Security Guard;
- the National Strategy of Cybersecurity 2017; and
- the White Paper on National Defense of the Mexican State.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

There is an industry-specific risk in certain sectors: financial; telecommunications; and health, not only in the private sector, but also at the governmental level. The National Security Guard Act, in November 8, 2019, which allows Mexican authorities to rule judicial decisions to intervene private communications for National Security purposes, anticipated the replacement of the Center of Investigation and National Security by the newly created National Intelligence Center, a Mexican intelligence agency controlled by the Ministry of Security and Civilian Protection, the main purpose of which is to preserve the State's integrity, stability and endurance. This was a radical structural change in the Mexican government as the former intelligence agency used to be under the control of the Ministry of Interior, the purpose being the reinvention of the image of the agency as an authority focused on security instead of conducting "authorised" espionage. During 2019, the National Intelligence Center

hosted an official meeting where representatives of the National Bureau of Investigation and the Department of Justice agreed with the Mexican government on a programme to coordinate efforts to reinforce the exchange of information concerning cybersecurity, including best practices to cope with activities that pose a risk for Mexico and the USA (i.e. financial, telecommunications and health, not only in the private sector, but also at the governmental level).

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

According to Mexican law (specifically, the Data Protection Law), organisations are compelled to implement corrective, preventive and improvement measures to make security measures adequate to avoid a breach. Organisations should be able to differentiate between material and non-material harm under Mexican laws by conducting a risk analysis. Material harm should be prioritised over non-material harm and will always depend on the business, scope, context and processing of the data compromised in the incident. Industry-specific risk identification of material and non-material harm is thus crucial for all companies facing a cybersecurity incident. Certain sectors, such as healthcare and banking, should provide companies with the required latitude to adapt their own internal policies. Compromising the security of databases, sites, programs or equipment (and this may include failure to implement required security measures) constitutes an administrative infringement of the Data Protection Law, which could be sanctioned with fines of up to Mex$25.6 million, a fine that may be doubled if sensitive data is compromised.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

From those incidents involving personal data, the Data Protection Law does not contain any obligation to the National Institute of Transparency, Access to Information and Protection of Personal Data ("INAI") about potential or actual incidents, including cyber threat or cyber-attacks. If the incident compromised personal data of identifiable individuals, then the business (understood as a data controller) must evaluate the breach through a risk assessment, implement the corrective, preventive and improvement actions to reinforce security measures, and determine if the event may result in prejudice to the property or non-pecuniary rights of the data subjects; if so, it should notify the affected parties. Under the Data Protection Law, security breaches occurring at any stage of processing personal data must be reported immediately by the data controller to the data owner, so that the latter can take appropriate action to defend its rights. There is no official format to notify breaches; however, the Data Protection Law and its regulations provide that the notification must include, at least, the nature of the breach, the personal data compromised, corrective actions implemented immediately by the data controller, recommendations concerning measures for the data owner to protect its interests after the breach and the means available for the data owner to obtain more information on the breach.

On the other hand and pursuant to article 106 of the Securities Market Law and its general provisions, listed entities are compelled to report to the National Banking and Securities Commission ("CNBV") all relevant events that may affect the value of its assets, including those involving incidents that impact a large amount of personal information, regardless of the cause of such events and including, of course, breaches of contracts, negligence or violation of other statutes such as the Data Protection Law.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Rules for reporting threats of breaches that may involve the unauthorised use of personal data are contained in the Data Protection Law. These Regulations provide that the data controller must inform only the data subject, not the federal regulator or other authority. As per the timeline, the regulations only provide that this notification should be conducted immediately, and after assessing whether the breach significantly affects the property or non-pecuniary rights of the data subjects upon having conducted an exhaustive review of the magnitude of the breach, so that the prejudiced data subjects may act appropriately.

There is no official format to notify breaches related to data privacy matters; however, the Data Protection Law and its regulations provide that the notification must include, at least, the nature of the breach, the personal data compromised, corrective actions implemented immediately by the data controller, recommendations concerning measures for the data owner to protect its interests after the breach and the means available for the data owner to obtain more information on the breach. Failure to comply with reporting obligations constitutes an administrative infringement to the Data Protection Law and may trigger fines that increase in cases of repeated infringements.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The Applicable Laws empower the following authorities to investigate an Incident: (i) the General Attorney Office; (ii) Public Prosecutors; (iii) the CNBV; (iv) the INAI; and (v) the Federal Telecommunications Institute ("IFT"). Public Prosecutors in Mexico are in charge of investigating cyber activities and to resolve them, a cyber police service has been created to follow up on crimes or unlawful activities committed through the internet. Complaints directed to the cyber police can be submitted via its website, by phone or through a Twitter or email account; in addition, the Federal Police has created a scientific division called the National Centre for Cyber-Incidents Response, specialising in providing assistance to the victims or claimants of cyber threats and cyber-attacks. In the case of data

protection, the INAI may conduct investigations to follow up personal data matters. Regarding telecommunications, the IFT is in charge of this sector.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

There is no single framework for non-compliance with notice requirements and penalties in Mexico; they will depend heavily on the relevant law and regulator, for example:

- Failure to comply with reporting obligations constitutes an administrative infringement of the Data Protection Law and may trigger fines that increase in case of repeated infringements.
- Failure to comply with reporting obligations of relevant events under the Securities Market Law may trigger the imposition of injunctive measures or the temporary suspension of the registry of securities' issuer.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

As of April 2020, the INAI has sanctioned many companies in cases involving violation of the Data Protection Law, most of them involving cybersecurity issues, to the extent that such authority has imposed fines for up to US$21 million in the last nine years. Entities devoted to financial services have been fined with almost US$12 million, followed by entities related to the communication industry, which fines amount US$2.5 million.

According to INAI and figures obtained from the official source of the National Commission for the Protection and Defence of Users of Financial Services, Mexico takes the eighth place in identity theft worldwide; 67% of those reported cases are due to the loss of documents, 63% for robbery, and 53% for information taken directly from credit accounts. During the third quarter of 2017, cyber fraud grew by 102% compared with the same period in 2016, representing a proportion from 13% to 51% per year. In 2018, 49,843 claims were filed upon identity theft and only 54% were decided in favour of the claimant. In addition, Mexico takes the second place in Latin America, with the greatest number of cyber-attacks to mobile devices.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Generally, yes.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Generally, yes.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Generally, yes.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Generally, yes, if organisations inform in advance that they will take these measures and obtain the proper consent from employees in order to prevent the unauthorised violation of private communications.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Generally, no, other than the restrictions already provided in the Industrial Property Law and the Copyright Law.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, according to the Data Protection Law, data controllers have to implement technical, physical and administrative measures in order to protect personal data from damage, loss, alteration, destruction, unauthorised use, access or processing.

The Federal Criminal Code and the Law on Negotiable Instruments and Credit Operations also include penalties to prevent criminal offences or violation of cybersecurity measures.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Yes. Such requirements are found under the Law on Negotiable Instruments and Credit Operations, the Credit Institutions Law, the Securities Market Act and the Federal Criminal Code, among other official regulations and guidelines.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

There is not a single framework, nor penalties for non-compliance with: prevention; mitigation; response to incidents amounting to a breach of directors; or officers' duties in Mexico. This will depend heavily on the relevant law.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

There is no single framework providing for requirements to designate a CISO or equivalent; establishing incident response plans, conducting risk assessments and performing vulnerability tests will depend heavily on the Applicable Law and industry. When personal data is involved, the appointment of a data privacy officer would then be required, as well as the implementation of other measures to avoid risks (including cyber risks).

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Requirements will depend heavily on the relevant law and especially whether the risk constitutes a relevant incident. Please refer to questions 2.4 and 2.6 above.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

According to article 32 of the Federal Criminal Code, organisations and companies are civilly liable for the damages caused to third parties by crimes committed by their partners, managers and directors. The state is similarly liable for the crimes committed by its public officials.

The Federal Civil Code provides a standard of civil liability established in article 1910, which provides that a party that illegally causes harm to another person shall be obliged to repair the damage, unless he/she proves that the damage was produced as a consequence of the victim's guilt or negligence.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

This is not applicable.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

This is not applicable.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Generally, yes.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Generally, no.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The Applicable Laws empower the following authorities to investigate an Incident: (i) the General Attorney Office; (ii) public Prosecutors; (iii) the INAI; and (iv) the IFT.

Public Prosecutors in Mexico are in charge of investigating and resolving cyber activities; a cyber police service has been created to follow up on crimes or unlawful activities committed through the Internet. Complaints directed to the cyber police can be submitted via its website, by phone, or through a Twitter or email account; in addition, the Federal Police have created a scientific division called the National Centre for Cyber-Incidents Response, specialised in providing assistance to the victims or claimants of cyber threats and cyber-attacks.

In the case of data protection, the INAI may conduct investigations to follow up personal data matters. The IFT is in charge of the telecommunications sector.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

This is not applicable in Mexican law.

Current Firm Contact

This chapter was authored by Begoña Cancino Garín, who has now left Creel, García-Cuéllar, Aiza y Enríquez. For any enquiries, please contact Gaby Finkel by phone on +52 55 4748 0624 or by email at gaby.finkel@creel.mx. Gaby Finkel is counsel in the Mexico City Office. She is an experienced attorney with more than 29 years' experience practising in the transactional and contractual fields of intellectual property, corporate law and privacy and data protection, both nationally and internationally. The combination of the practice as exercised from a law firm perspective, with extensive commercial knowledge, as well as a strategic and innovative viewpoint required for business solutions, has resulted in important achievements in favour of her clients. Having practised both in Mexico and the USA, she has experience with national and international clients, crafting agreements of a diverse nature (including licensing, merchandising, distribution, franchises and services, as well as entertainment rights, trademarks and copyrights), as well as the drafting and revision of internal privacy policies, privacy notices and terms and conditions.

Begoña Cancino Garín was formerly a partner in the Mexico City office. Her practice has focused on Intellectual Property, Data Privacy, Regulatory and Administrative Litigation. From the standard IP front, Begoña has counselled clients from all kinds of industries with the protection and enforcement of their IP rights in Mexico, also assisting with the transfer of IP portfolios within the context of complex corporate transactions involving all sorts of IP rights (such as trademarks, copyrights and appellations of origin). Begoña has also provided assistance with her legal advice on regulatory and advertising, assessing our clients to comply with all applicable provisions with COFEPRIS and PROFECO. She has represented clients in all types of administrative litigation proceedings, in general, concerning advertising, health, environmental and, of course, IP matters, before administrative authorities and federal judicial courts. Pursuant to the data privacy aspects of her practice, Ms. Cancino has counselled clients from multiple industries in the drafting and implementation of internal policies, privacy notices and specific legal concerns, not only regarding client daily operations, but also within the context of cross-border transactions and internal investigations for compliance.

With over 85 years of history, Creel, García-Cuéllar, Aiza y Enríquez is a leading full-service corporate law firm with an unwavering commitment to excellence. We have an established reputation for delivering creative, specialised and responsive legal advice on the most complex and innovative matters in Mexico for the most sophisticated and demanding clients. Our practice is based on the philosophy that a client is best served by legal advice designed to anticipate and avoid problems, rather than respond to them. Our goal is to be the law firm of choice for clients with the most demanding transactions and projects, and, in such endeavour, become a strategic service provider to them, by offering the type of legal advice that gives clients certainty and peace of mind. We view our role as one of adding value to our clients and providing them with certainty and peace of mind. As such we strive to become their strategic service provider.

www.creel.mx

CREEL GARCÍA-CUÉLLAR AIZA Y ENRÍQUEZ

Norway


Stian Hultin Oddbjørnsen


Ove André Vanebo


Iver Jordheim Brække


Mari Klungsøyr Kristiansen

CMS Kluge

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Intrusion into a computer system, hacking included, constitutes a criminal offence under section 204 of the **Penal Code** of 20 May 2005. The provision states that a person who, by breach of a protective measure or other illicit means, obtains access to a computer system or part thereof, may be given a penalty of a fine or imprisonment for a term not exceeding two years. An example of a prosecution under this section is found in the Supreme Court Judgment HR-2020-2056-A, where a person was given a sentence of imprisonment for one year (with nine months being conditional).

As for the rest of the following activities, hacking would primarily be considered a criminal offence to be investigated by the prosecuting authority. Consequently, administrative offences are less likely.

Denial-of-service attacks
Denial-of-service attacks will typically fall within the scope of section 206 of the **Penal Code**, which stipulates that creation of a risk of operational disruption is a criminal offence. Under this section, a person who, by transferring, damaging, deleting, degrading, modifying, adding or removing information, illicitly creates a risk of interruption or significant disruption of the operation of a computer system, may be given a penalty of a fine or imprisonment for a term not exceeding two years.

Phishing
Phishing constitutes a criminal offence under section 202 of the **Penal Code**, which criminalises the violation of identity. Under this provision, a person who, *inter alia*, illicitly gains possession of another person's proof of identity or an identity that is easily mistakable for the identity of another person, with intent to:

a) make an illicit gain for himself/herself or for another person; or
b) cause another person loss or inconvenience,

may be punished with a fine or imprisonment for a term not exceeding two years.

An example of a prosecution under this section is found in Supreme Court Judgment HR-2020-1352-A, where a person was given a sentence of imprisonment of one year and six months. However, this case also involved fraud by use of the other person's proof of identity, which added to the sentence.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infection of IT systems with malware constitutes a criminal offence under section 206 of the **Penal Code**. This is the same section that applies to denial-of-service attacks, mentioned above.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Section 201 of the **Penal Code** criminalises an act where any person who, with intent to commit a criminal act, illicitly makes available to another person:

a) a password or other information that may provide access to computerised information of a computer system; or
b) a computer program, or something else that is particularly suitable for committing criminal acts, targeting computerised information or computer systems.

Such distribution or sale is penalised with a fine or imprisonment for a term not exceeding one year. As section 16 of the **Penal Code** also criminalises attempts to offences that may be punishable by imprisonment for a term of one year or more, the offering for sale of such tools could also be considered a criminal act.

Possession or use of hardware, software or other tools used to commit cybercrime
The possession of tools to commit cybercrime is also criminalised by section 201 of the **Penal Code**, mentioned directly above, as this provision also applies to cases where the person produces, procures or possesses the mentioned authentication details, computer programs, etc.

When it comes to the use of the hardware, software or other tools used to commit cybercrime, it is not the *use* that is criminalised, but rather the more specified acts mentioned here in question 1.1. This includes violation of identity under section 202, intrusion into a computer system/hacking under section 204, violation of the right to private communication under section 205, risk of operational disruption under section 206, and the like.

Identity theft or identity fraud (e.g. in connection with access devices)
The above-mentioned section concerning violation of identity in the **Penal Code**, section 202, which criminalises phishing, also criminalises identity theft or identity fraud. In addition to criminalising the act where a person illicitly gains possession of another person's proof of identity or an identity that is easily mistakable for the identity of another person, the provision criminalises the illicit *use* of such identity.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
The **Penal Code**'s "regular" theft section, section 321, only applies to tangible property, and there is no general *electronic* theft provision as such. However, there are different provisions that may apply to the electronic theft of specific types of information. *Inter alia*, section 208 of the **Penal Code** section 208 penalises the illegal appropriation of a business secret with a fine or imprisonment not exceeding one year, and section 203 provides a similar penalty for the possession of a decoding device giving access to a protected communication service.

In addition, the **Copyright Act** of 15 June 2018, section 79, *cf.* sections 80 and 3, provides that streaming is punishable with a fine or imprisonment for a term not exceeding three years. Such punishment does, however, require that it was evident that the streaming was breaking the law and that the use of the illegal source was capable of significantly damaging the financial interests of the author.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
To our knowledge, there are no provisions directly addressing unsolicited penetration testing if the testing itself does not harm the system or its owner. However, if the access to the system is a result of intrusion into a computer system, such action is punishable under the above-mentioned section 204 of the **Penal Code**.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Another activity considered a criminal offence under Norwegian law is the violation of the right to private communication. Section 205 of the **Penal Code** provides, *inter alia*, that a fine or imprisonment for a term not exceeding two years may be imposed on any person who illicitly breaches a protective measure and thereby gains access to information transmitted using electronic or other technical means.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The conditions for extraterritorial application of the **Penal Code** are set forth in section 5. Such application *usually*, although with several exceptions, requires:

a) a personal nexus to Norway (being if a person is a Norwegian national, domiciled in Norway or acts on behalf of an enterprise registered in Norway); and
b) that the offence is also punishable under the law of the country in which it is committed.

In addition, the prosecution of acts committed abroad are limited to cases where such prosecution is considered "in the public interest". Consequently, the above-mentioned offences may be given extraterritorial application.

What might, however, be more relevant for cybersecurity offences is how section 7 relatively openly regulates when an act is to be considered to have taken place in Norway, thereby not actualising the question of extraterritorial application. This provision provides that where the punishability of an act is contingent on or affected by an actual or intended effect, the act is also deemed to have been committed at the place where the effect has occurred or was intended to be caused. Hence, where the effects of one of the above-mentioned offences occur in Norway, e.g. where the intrusion into a computer system in Norway is executed from another country, such act is punishable under Norwegian law.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Section 78 of the **Penal Code** lists nine different mitigating factors that are to be considered when deciding the sentence of a criminal act. The most relevant factors in relation to the above-mentioned offences are where: (1) the offender has made an unreserved confession; and (2) the offender has prevented, reversed, or limited the harm or loss of welfare caused by the offence, or sought to do so.

As for exceptions, there is no general rule stating that "ethical" intent excepts an act from being punished when it otherwise meets the conditions of the criminal offence. On the contrary, the main rule is that exceptions are not to be given. However, they could still be considered in extraordinary circumstances.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

There is no general Applicable Law especially dedicated to cybersecurity in Norway. The relevant Applicable Laws that regulate cybersecurity are fragmented and often sector-specific. We have listed *some* of the essential Applicable Laws regarding cybersecurity below:

a) All processing of personal data is subject to the **General Data Protection Regulation** (**GDPR**) (Regulation (EU) 2016/679) and the **Personal Data Act** of 15 June 2018.
b) The **National Security Act** of 1 June 2018 aims, *inter alia*, to prevent, detect and counteract activities threatening national sovereignty, including regulations on information security.
c) The **Electronic Communications Act** of 4 July 2003 and the **Electronic Communications Regulation** of 16 February 2004 aim to give secure and modern communication services to the public.
d) The **Energy Act** of 29 June 1990 and the **Power Supply Preparedness Regulation** of 7 December 2012 aim to secure power supply and include regulations on information security and safety measures for control systems.
e) The **Regulation on the Use of Information and Communication Technology** of 21 May 2003 (**ICT Regulation**) within the financial services regulates, *inter alia*, the use and security of ICT systems in that sector.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The Applicable Laws mentioned in question 2.1 are all applicable to critical infrastructure, or operators of essential services

if the provided service falls within the scope of the Applicable Laws. However, there are no provisions in the Applicable Laws that are specifically designed to solely regulate Incidents in this regard. The provisions are often written in a way that allows one single statutory provision to cover many types of circumstances, including Incidents regarding cybersecurity.

An example is **GDPR** article 24 (1), which states that the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the **GDPR**. The article will be relevant for all organisations processing personal data, including activities related to critical infrastructure or similar activities that require such processing.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

All the above-mentioned Applicable Laws in question 2.1 require organisations to monitor, detect, prevent and mitigate Incidents.

Organisations that process personal data and can be defined as a data controller or processor must follow the regulations under the **GDPR**. Data controllers and processors are, among other statutory regulations in the **GDPR**, required to follow the principles relating to the processing of personal data according to **GDPR** article 5. The organisations are also obligated to implement technical and organisational measures to ensure a level of security appropriate to the risk of the data processing.

Organisations that fall within the scope of the **National Security Act** are required to carry out risk assessments and implement proportionate security measures.

The **Electronic Communications Act** requires organisations to implement necessary security measures for the protection of communications and data.

Energy suppliers and other organisations that fall within the scope of the **Energy Act** are obligated to implement necessary security measures for all processing of information relating to power supplies. Organisations are also, *inter alia*, responsible for protecting sensitive information and preventing access to non-legitimate users.

Organisations that fall within the scope of the **ICT Regulation** are required to develop procedures to ensure the protection of equipment, systems, and information relevant to the activities in the organisation. The organisations are also required to do risk analyses and establish criteria for the acceptable risk associated with the use of the ICT systems.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

All organisations under the Applicable Laws described in question 2.1 are required to report information to authorities related to Incidents or potential Incidents. However, not all of the Applicable Laws set out the nature and scope of the information that is required to be reported. We have written an overview of the relevant authorities to which the information is required to be reported below in question 2.6.

Organisations that process personal data according to the **GDPR** shall, without undue delay, notify the personal data breach to the supervisory authority. The reporting obligation is triggered for any personal data breach unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The information the organisations are required to report shall at least include the nature of the personal data breach, the name and contact details of the data protection officer or other contact point, a description of the likely consequences of the personal data breach and a description of the measures taken to address the personal data breach.

In cases where they have been affected by security-threatening activities or if there is a well-founded suspicion of security-threatening activities, organisations that fall within the scope of the **National Security Act** are required to immediately notify the security authorities.

The **Electronic Communications Act** requires organisations to notify authorities if there are security breaches or risks of such. However, it is not necessary to notify the authorities if it is possible to document that satisfactory technical protection measures have been implemented for the data covered by the breach of security.

Energy suppliers and other organisations that fall within the scope of the **Energy Act** are required to give the authorities any necessary information for the implementation of provisions pursuant to the Act. This can include information about Incidents or potential Incidents.

Organisations that fall within the scope of the **ICT Regulation** are required to inform the authorities without undue delay about Incidents that result in a significant reduction in functionality resulting from breaches regarding confidentiality, integrity or access to ICT systems.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Some of the Applicable Laws described in question 2.1 require organisations to report information related to Incidents or potential Incidents to any affected individuals.

The **GDPR** requires organisations that process personal data and are considered data controllers to inform the data subject of personal data breaches that are likely to result in a high risk to the rights and freedoms of the affected individuals. The information the organisations are required to report shall at least include the nature of the personal data breach, the name and contact details of the data protection officer or other contact point, a description of the likely consequences of the personal data breach and a description of the measures taken to address the personal data breach.

Organisations that fall within the scope of the **Electronic Communications Act** must notify individuals of significant risks of security breaches, including security breaches that have damaged or destroyed data, or violated the individual's right to privacy. However, the organisations are not obligated to report Incidents to affected individuals if the organisations are able

to prove that appropriate security measures have been implemented on the data affected by the Incident. There are no provisions in the Act that describe the nature and scope of information required to be reported.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The following regulators are responsible for enforcing the requirements according to the Applicable Laws described in question 2.1:

a) The **Norwegian Data Protection Authority** (**NDPA**) is responsible for enforcing provisions in the **GDPR**.
b) The **Norwegian National Security Authority** is responsible for enforcing the provisions in the **National Security Act**.
c) The **Norwegian Communication Authority** (**NCA**) is responsible for enforcing the **Electronic Communications Act** and the **Electronic Communications Regulations**.
d) The **Energy Directorate** is responsible for enforcing the provisions in the **Energy Act**.
e) The **Norwegian Financial Supervisory Authority** is responsible for enforcing the provisions in the **ICT Regulation**.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

We have described how the regulators mentioned in question 2.6 can sanction organisations below:

a) The **NDPA** can impose administrative fines up to EUR 20 million or, in the case of an undertaking, 4% of the total worldwide annual turnover. Infringements of the reporting requirements under the **GDPR** are limited to EUR 10 million or, in the case of an undertaking, 2% of the total worldwide annual turnover.
b) The **Norwegian National Security Authority** can impose coercive fines and administrative fines for violations of the **Security Act**.
c) The **NCA** can impose coercive fines and administrative fines for violations of the **Electronic Communications Act** and the **Electronic Communications Regulations**.
d) The **Energy Directorate** can impose coercive fines and administrative fines.
e) The **Norwegian Financial Supervisory Authority** can impose coercive fines.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The authorities mentioned in question 2.6 have, to our knowledge, not taken any enforcement action in cases of non-compliance where an organisation has been exposed to a cyber-attack, or any other enforcement action in direct relation to cybersecurity. However, the authorities have on several occasions fined organisations in cases of non-compliance with the Applicable Laws mentioned in question 2.1. The two cases mentioned below received a lot of media attention in Norway.

Nine hospitals received a fine of NOK 800,000 each from the **NDPA** in 2017. The hospitals outsourced ICT operations and processing of data concerning health to a processor in Bulgaria. The **NDPA** concluded that the outsourcing was not in compliance with the obligations under the **GDPR**, including the provisions regarding safety management, risk assessments and access management.

A Norwegian municipality was fined NOK 1.6 million by the **NDPA** in 2019 after a student had gained unauthorised access to a school's ICT systems, uncovering severe flaws in the security systems of the municipality including personal information.

The **NCA** sanctioned a telecom provider with a fine of NOK 11 million because the telecom provider failed to implement adequate security measures to prevent unauthorised access to the computer system that operates parts of the Norwegian emergency network.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

There are no specific prohibitions against the use of beacons and organisations are permitted to use beacons under Norwegian law. However, as IP addresses would be considered personal data under Norwegian law if the organisation collecting the IP address has the means to identify the person using the IP address, the use of beacons will require the organisation to have a legal basis under **GDPR** article 6.

The use of beacons could also be regulated by section 2-7b of the **Electronic Communications Act**, regulating the use of cookies. This section provides that the user of the computer in question must be informed of and consent to the use of cookies. Such consent could, however, be provided through the user's browser settings.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

As is the case for beacons, there are no specific prohibitions against the use of honeypots. Consequently, organisations are permitted to use honeypots under Norwegian law as long as such use is compliant with the above-mentioned cybersecurity legislation.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)

The use of sinkholes is also permitted under Norwegian law, as long as such use is compliant with the above-mentioned cybersecurity legislation.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

As a rule, the **Regulation on Employers' Access to Email Inboxes and Other Electronically Stored Material** of 2 July 2018 provides that organisations are not permitted to monitor or intercept the employees' email accounts or internet usage. Section 2 in the mentioned regulation does, however, allow for

organisations to access the email accounts when it is considered necessary to protect the daily management of the organisation or other legitimate interest of the organisation. The same section also allows the organisation to access the employees' internet usage when it is considered necessary to manage the organisation's network or to identify or solve a security breach in the network.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

There are no restrictions as to the import or export of technology designed to prevent or mitigate the impact of cyber-attacks under Norwegian law.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Organisations must adhere to the legal requirements in Norway, and market practice in a specific sector that deviates from the requirements under the Applicable Laws will not be considered legitimate.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Some of the Applicable Laws mentioned in question 2.1 regulate specific market sectors:

a) Telecom providers and other organisations that operate in the telecommunications sector are subject to the **Electronic Communications Act** and the **Electronic Communications Regulation**.
b) The **Energy Act** applies to organisations that produce, transform, transfer, sell or distribute energy.
c) Banks, financial undertakings, and other organisations that operate within the financial sector are subject to the **ICT Regulation**.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

The failure by a company to prevent, mitigate, manage or respond to an Incident, primarily if the company is required by law to perform such activities (like the requirements mentioned under section 2) would normally be considered a breach of the board's duties under the **Limited Liability Company Act** of 13 June 1997, and the **Public Limited Liability Company Act** of 13 June 1997 sections 6-12 and/or 6-13. The officers' duties are normally more limited. However, in certain situations, depending on multiple factors, the failure might also constitute a breach of the officers' duties.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

The companies required to implement the measures listed in a)–d) are corresponding to the companies that fall within the scope of the statutes and regulations listed in question 2.1. However, not all measures are required under all acts. In summary, the following measures are required:

a) The **Power Supply Preparedness Act** section 2-2 provides that energy suppliers are required to designate a CISO; under the **ICT Regulation** section 2, financial undertakings are required to designate persons that are responsible for the different parts of their ICT systems, including information security; and under **GDPR** article 37, some companies are required to designate a data protection officer.
b) The **ICT Regulation** sections 2 and 5 and the **Power Supply Preparedness Act** sections 2-4 and 6-4 state that, respectively, electronic communication providers and financial undertakings are required to establish a written Incident response plan or policy. In addition, most companies processing personal data are required to establish such plans under **GDPR** article 32.
c) The **ICT Regulation** section 3 and the **Power Supply Preparedness Act** section 2-3 state that the above-mentioned companies are required to conduct cyber risk assessments. Under **GDPR** article 35, this also applies to most companies processing personal data.
d) The requirement to perform penetration tests or vulnerability assessments would in some cases follow from the requirements mentioned in c).

In addition, the **Electronic Communications Act** section 2-7 more generally provides that telecom providers are to implement the security measures necessary to secure their data. Such measures could include all the above, depending on the situation. The measures could also be required under the **Security Act** for companies that, due to a decision based on section 1-3 of the Act, have been decided to fall within the scope of the Act.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Companies are not under any general obligation to specifically disclose any information in relation to cybersecurity requirements or Incidents under Norwegian law, other than those mentioned in section 2.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Proceedings related to cybersecurity are typically not the subject of private civil action lawsuits. It is more common that one of the responsible authorities mentioned in question 2.6 issues an

administrative fine to a private subject. The private subject can then take the administrative fine to court if they disagree with the decision made by the authorities.

However, we believe that an increase in civil lawsuits between data subjects and organisations that have violated the data subject's rights under **GDPR** may occur. This is because it follows from **GDPR** article 82 that any data subject who has suffered material or non-material damage as a result of an infringement of the **GDPR** shall have the right to receive compensation from the controller or processor for the damage suffered.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

There are, to our best knowledge, no examples of published civil or other private actions that have been brought into Norwegian jurisdiction in relation to Incidents.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Any person who negligently or wilfully causes an Incident may under the Norwegian law of torts be held liable for any foreseeable loss that has occurred due the negligent or wilful act.

However, the Norwegian law of torts will only be applicable if there is no other relevant law or contract that regulates the same matter. For example, a data subject cannot claim damages based on tort law if the data subject can claim compensation according to the rules in the **GDPR**.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Organisations in Norway are permitted to take out insurance against Incidents.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

We are not familiar with any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The most relevant investigatory powers are set forth in the **Criminal Procedure Act** of 22 May 1981. Under this Act, the police, the prosecuting authority and/or the court – depending on the severity of the investigatory power – may, *inter alia*:

a) conduct a search of a data system and order any person with access to the system to give the encryption keys necessary to access the system. Such order could also include forced biometrical authentication;
b) order the expeditious preservation of specified computer data that has been stored by means of a computer system, including from providers of electronic communication services and networks;
c) seize evidence, including tangible property and electronically stored information; and
d) secretly put a suspect's computer under surveillance and thereby gather information through technical means, such as secretly installing a software on the computer, utilising the suspect's credentials if such are gathered or entering the computer's system through hacking.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Applicable Laws do not require organisations to implement backdoors in their IT systems. As for requirements for organisations to provide law enforcement authorities with encryption keys, such requirements exist (see question 8.1).

Stian Hultin Oddbjørnsen is specialised within "tech law". Stian is a recognised and ranked lawyer within TMT. Stian advises both public and private entities on, *inter alia*, regulatory, and cybersecurity-related matters in this field of law. Furthermore, Stian has extensive knowledge and experience in procurement, contract drafting and negotiations within digitalisation projects. Stian is also a proven litigator and handles disputes and court cases. He has also acted as a deputy judge in Drammen District Court for a period of two-and-a-half years, handling both civil and criminal cases. He regularly publishes articles on tech law and often acts as a lecturer on such topics.

CMS Kluge
Bryggegata 6
0250 Oslo
Norway

Tel: +47 957 89 414
Email: sho@kluge.no
URL: www.kluge.no

Ove André Vanebo assists private and public clients with data privacy, labour law, cybersecurity and dispute resolution. He has wide-ranging experience with privacy matters, such as surveillance, storing and further processing of personal data and data breaches. He also frequently acts as a lecturer and has written numerous articles about privacy and data protection.

CMS Kluge
Bryggegata 6
0250 Oslo
Norway

Tel: +47 915 49 378
Email: ove.vanebo@kluge.no
URL: www.kluge.no

Iver Jordheim Brække is a part of Kluge's tech team. He primarily assists clients with advisory work within technology, public procurement and data privacy.

CMS Kluge
Bryggegata 6
0250 Oslo
Norway

Tel: +47 464 24 959
Email: iver.jordheim.brekke@kluge.no
URL: www.kluge.no

Mari Klungsøyr Kristiansen is a part of Kluge's tech team. She primarily assists clients with dispute resolution and advisory work within technology and public procurement.

CMS Kluge
Bryggegata 6
0250 Oslo
Norway

Tel: +47 479 03 123
Email: mari.klungsoyr.kristiansen@kluge.no
URL: www.kluge.no

CMS Kluge is a full-service law firm with offices in Oslo, Stavanger, Bergen and Hamar. We offer comprehensive advice and assistance within all major fields of business law and are one of the leading law firms in Norway. CMS Kluge's practice group within TMC offers a wide range of services to both private and public clients within these fields of law. CMS is a future-facing law firm. With more than 70 offices in over 40 countries and 4,800+ lawyers, we combine deep local market understanding with a global overview. With a team of data protection and cybersecurity specialists totalling just over 200, we incorporate our next-generation mindset in all our advice – from cyber-breach response, to regulatory investigations and follow-on claims, as well as compliance.

www.kluge.no

Poland


Mateusz Borkiewicz


Grzegorz Leśniewski


Jacek Cieśliński

Leśniewski Borkiewicz & Partners (LB&P)

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Criminal offence: Hacking is a criminal offence under Section 267 of the Polish Criminal Code. Anyone who, without being authorised to do so, acquires access to information not intended for him or her, by, *inter alia*, connecting to a cable transmitting information or by breaching electronic, magnetic or other special protection for that information, is liable to a fine (up to PLN 1.08 million), restriction of liberty or imprisonment for up to two years. This also applies to anyone who acquires access to any part of a computer system without being authorised to do so.

Administrative offence: Unauthorised access to information may constitute an act of unfair competition. This applies in particular to cases where such action is aimed at violating the interests of another entrepreneur (e.g. unauthorised access to information of economic value that may constitute a breach of the business secret of another entity). In such cases, hacking may be of interest to the President of the Office of Competition and Consumer Protection. This offence has a penalty of up to 10% of the annual turnover.

If unauthorised access to information includes information constituting personal data, a violation of the General Data Protection Regulation (GDPR) is also likely; this has a penalty of up to EUR 20 million or, in the case of an enterprise, up to 4% of its total annual global turnover (whichever is higher).

Denial-of-service attacks
Criminal offence: Denial-of-service (DoS) attacks are a criminal offence under Section 269a of the Polish Criminal Code. Anyone who, without being authorised to do so, by transmitting, damaging, deleting, destroying or altering information data, significantly disrupts a computer system or telecommunications network is liable to imprisonment for up to five years. In some cases, DoS attacks can also constitute offences under Sections: 268 (hindering access to information); 268a (damaging databases due to interfering or preventing automatic collection and transmission of data or hindering access to data); and 269 (if the offence regards data that is of particular significance for national defence, transport, safety or the operation of the government or any other state authority or local government).

Administrative offence: DoS attacks may constitute:

- acts of unfair competition (i.e. restricting access to the market for another entrepreneur, in accordance with the Suppression of Unfair Competition Act of 16 April 1993); or
- unfair market practice, i.e. making it difficult for consumers to access services (in accordance with the Act on Combatting Unfair Market Practices).

In both cases, DoS attacks may be of interest to the President of the Office of Competition and Consumer Protection. The penalty for this offence is a fine of up to 10% of the annual turnover.

Phishing
Criminal offence: Phishing is a criminal offence under Section 287 of the Polish Criminal Code. Anyone who, in order to achieve material benefits or to inflict damage upon another person, affects the automatic processing, collection or transmission of data or changes, deletes or introduces new entries, without being authorised to do so, is liable to imprisonment for up to five years. If phishing leads to identity theft or fraud, it may also be considered an offence under Section 190a of the Polish Criminal Code (see more below).

Administrative offence: Cases where phishing is aimed at violating the interests of another entrepreneur, i.e. in order to: illegally obtain information covered by the business secret of another entity; disseminate false information about another entity; or restrict access to the market of another entity (e.g. obstructing the transaction's execution), it may be of interest to the President of the Office of Competition and Consumer Protection. A penalty of up to 10% of the annual turnover will apply.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Criminal offence: Infecting IT systems with malware is a criminal offence under Section 287 of the Polish Criminal Code (for quotation, see 'Phishing' above). Moreover, according to Section 269 of the Polish Criminal Code, anyone who destroys, deletes or changes a record on a computer storage media that is of particular significance for national defence, transport, safety or the operation of the government or any other state authority

or local government, or that interferes with or prevents the automatic collection and transmission of such information, is liable to imprisonment for up to eight years. Infection of IT systems with malware may be also a criminal offence if it results in at least one of the following: unauthorised access to information; destruction of information; damage to databases; DoS; computer fraud (i.e. phishing); or disruption of work on a network.

Administrative offence: If infection of IT systems with malware results in: unauthorised access to information; destruction of information; damage to databases; DoS; computer fraud (i.e. phishing); or disruption of work on a network, it may constitute an administrative offence, including: a violation of the GDPR (e.g. if it concerns personal data), which has a penalty of up to EUR 20 million or, in the case of an enterprise, up to 4% of its total annual global turnover (whichever is higher); or an act of unfair competition (if the aim is to violate the interests of another entrepreneur), which has a penalty of up to 10% of the annual turnover.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

Criminal offence: Such actions are criminal offences under Section 269b of the Polish Criminal Code. Anyone who creates, obtains, transfers or allows access to hardware or software adapted to commit cybercrime (e.g. damaging databases, preventing automatic collection and transmission of data or hindering access to data) is liable to imprisonment for up to five years.

Administrative offence: Such actions may also be of interest to the President of the Office of Competition and Consumer Protection, with a penalty of up to 10% of the annual turnover. In particular, the production, import, distribution, sale or rental, for commercial purposes, of prohibited devices (within the meaning of the provisions on the protection of certain services provided electronically based on conditional access) constitute an act of unfair competition (art. 15b of the Suppression of Unfair Competition Act of 16 April 1993).

Possession or use of hardware, software or other tools used to commit cybercrime

Criminal offence: Anyone who creates, obtains, transfers or allows access to hardware or software adapted to commit the offences specified above, including computer passwords, access codes or other data enabling access to the information collected in the computer system or telecommunications network, is liable to imprisonment for up to three years.

Administrative offence: In order to commit the acts of unfair competition described in the above points, it is sufficient that a given action 'threatens' the interests of another entrepreneur (specific violations, e.g. access to the information covered by the business secret, are not a necessary element). It means that, in specific cases, the mere possession of hardware, software or other tools used to commit cybercrime could justify the actions of the President of the Office of Competition and Consumer Protection (a penalty of up to 10% of the annual turnover).

Identity theft or identity fraud (e.g. in connection with access devices)

Criminal offence: Identity theft or fraud is a criminal offence under Section 190a of the Polish Criminal Code. Anyone who pretends to be another person and uses his or her image, or other personal data, in order to cause property or personal damage, may be subject to imprisonment for up to three years.

Administrative offence: A designation of a company that may mislead customers as to its identity (e.g. by using a company name or other distinctive symbol previously legally used to designate another entity) constitutes an act of unfair competition (art. 5 of the Suppression of Unfair Competition Act of 16 April 1993) and may be of interest to the President of the Office of Competition and Consumer Protection (with a penalty of up to 10% of the annual turnover).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Criminal offence: Electronic theft is a criminal offence under Section 266 of the Polish Criminal Code. Anyone who, in violation of the law or an obligation accepted, discloses or uses information learned in connection with the function or work performed, or public, social, economic or scientific activity pursued, is liable to a fine, the restriction of liberty or imprisonment for up to two years.

Administrative offence: Undertaking such actions may, in certain circumstances, constitute a breach of business secrets and result in a number of civil law consequences, and if committed by other entrepreneurs, it may even result in the President of the Office of Competition and Consumer Protection carrying out proceedings (with a penalty of up to 10% of the annual turnover).

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Criminal offence: Unsolicited penetration testing is a criminal offence under Section 267 of the Polish Criminal Code. Anyone who, without being authorised to do so, acquires access to information not intended for him or her, by, *inter alia*, connecting to a cable transmitting information or by breaching electronic, magnetic or other special protection for that information, is liable to a fine (up to PLN 1.08 million), restriction of liberty or imprisonment for up to two years. This also applies to anyone who acquires access to any part of a computer system without being authorised to do so.

Unsolicited penetration testing may also constitute a criminal offence under Section 266 of the Polish Criminal Code – Electronic theft (described in the point above).

Administrative offence: The exploitation of an IT system without the permission of its owner may constitute an act of unfair competition (a breach of the business secret of another entity). In such cases, it may be of interest to the President of the Office of Competition and Consumer Protection, with a penalty of up to 10% of the annual turnover.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

1. Under Section 165, subsect. 1 point 4 of the Polish Criminal Code, anyone who puts the lives or health of many people or possessions in danger by affecting computerised data commits a separate crime and may be sentenced for up to eight years of imprisonment. If any offence is committed due to or in relation to the offences listed above, the offender may be found guilty of committing several offences by one act; if the offence is related to terrorism, the punishment may be even more severe.
2. The Polish legal system contains a number of regulations sanctioning threats to IT systems that do not result from external factors (such as hacking, phishing, etc.), but from the negligence of entrepreneurs using such systems (failure to meet certain security obligations imposed by law), i.e.:
   - National Cybersecurity System Act of 5 July 2018 (NCS) (NIS Directive implementation): a penalty of up to PLN 150,000, incl. for not carrying out a systematic risk assessment or not managing the risk of an Incident.
   - GDPR: a penalty of up to EUR 10 million and, in the case of an enterprise, up to 2% of its total annual

global turnover (whichever is higher), including for failure to implement security measures for IT systems adequately to the risk.
- Telecommunications Law of 16 July 2004: a penalty of up to 3% of the annual income, incl. for failure to implement technical and organisational IT security measures.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Criminal offences: All of the listed offences are included in the Polish Criminal Code and, although there are no specific regulations on extraterritorial application of these offences, the territorial application of the Polish Criminal Code depends on the place of the offence. The Polish Criminal Code (Sections 5 and 6, subsect. 2) is applicable when the offender acted or omitted an action to which they were obliged, or where the result occurred or should have occurred in accordance with the intention of the offender, or acted outside Poland but the result of one of the listed offences occurred in Poland, i.e. the offence affects IT systems located in Poland or systems used for providing services in Poland.

Administrative offences: The exterritorial application will depend on the context of the case, including the type of violation and the competent authority to investigate it. In most cases, the authorities will be able to take appropriate action against entities that have establishment in Poland or against actions that have or may have effects in Poland.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Yes, there are general principles set out in the Polish Criminal Code and applicable to all the offences specified in it (including the offences listed above), which allow for mitigating penalties:
- Section 59 – draw back – allows the court to draw back from imposing a penalty in case of milder offences.
- Section 60 – extraordinary mitigation of punishment – allows the court to extraordinarily mitigate the punishment in cases indicated in a statute or in particularly justified cases when even the mildest punishment would be incommensurably harsh.

Also, when it comes to administrative offences, Polish regulations provide mechanisms that allow the reduction of liability for illegal activities. Mitigating circumstances often include actions such as voluntary removal of the effects of a breach or cooperation with the authority.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

European Union – Key Applicable Laws:
1. Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.
2. Regulation (EU) 2019/881 on the European Union Agency for Cybersecurity (ENISA) and on information and communication technology cybersecurity certification – under this regulation, soon there will be a uniform system of certification of cybersecurity of ICT in the EU, allowing for easier verification of the level of cybersecurity provided by organisations.
3. Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market.
4. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).
5. Directive (EU) 2015/2366 on payment services in the internal market (PSD2).

Poland – Key Applicable Laws:
1. Criminal Code of 6 June 1997;
2. Labour Code of 26 June 1974;
3. Civil Code of 23 April 1964;
4. NCS (NIS Directive implementation);
5. Trust Services and Electronic Identification Act of 5 September 2016;
6. Data Protection Act of 10 May 2018;
7. Suppression of Unfair Competition Act of 16 April 1993;
8. Competition and Consumer Protection Act of 16 February 2007;
9. Telecommunications Law of 16 July 2004;
10. Counter-terrorism Act of 10 June 2016;
11. Crisis Management Act of 26 April 2007;
12. Payment Services Act of 19 August 2011;
13. Classified Information Protection Act of 5 August 2010; and
14. Recommendations and Instructions of the Financial Supervision Commission (KNF) concerning management of information technologies and security of the ICT environment.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The Network and Information Systems Directive is implemented in Poland by the NCS. However, there are some sectors of critical infrastructure that are wholly or partially regulated in other Applicable Laws: trust service providers; health service providers established by the Chief of Internal Security Agency or Chief of Foreign Intelligence Agency (i.e. Trust Services and Electronic Identification Act of 5 September 2016 and a set of regulations concerning some categories of health service providers); and telecommunications entrepreneurs referred to in the Telecommunications Law of 16 July 2004 (partially regulated in the NCS and partially in the Telecommunications Law – in relation to cybersecurity requirements and Incident reporting).

Financial service providers are also subject to additional obligations regulated in statutes, which are specific for different kinds of financial service providers, e.g. for payment service providers: Payment Services Act of 19 August 2011 (implementing PSD2) – please also see the answer to question 4.2.

The NCS exceeds the requirements of the NIS Directive by including public administration, and partially the telecommunications sector, into the scope of the regulation. The NCS makes public administration provide at least the same standard

of cybersecurity as operators of essential services and digital service providers, i.e. take measures to monitor, detect, prevent or mitigate Incidents at a similar level as operators of essential services and digital service providers.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes, organisations are required to undertake several activities to monitor, detect, prevent or mitigate Incidents. Under the NCS, operators of essential services shall implement a security management system for the information system used to provide the essential service that is relevant and proportionate to the estimated risk (having regard to the state of the art) and measures to prevent and minimise the impact of Incidents (examples are provided). A security audit of the information system must be carried out at least every two years. Under the NCS, digital service providers shall also face similar and relevant requirements.

In accordance with the Act on Provision of Electronic Services 2002, the service provider, in general, shall use appropriate cryptographic techniques.

In accordance with the Payment Services Act 2011, the provider, as part of the risk management system, takes risk mitigation measures and implements control mechanisms to manage risk through an effective Incident management procedure, including detection and classification of Incidents, including those related to ICT systems (e.g. strong user authentication).

In accordance with the GDPR, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (examples are given in Section 32, subsect. 1 of the GDPR).

In accordance with the Telecommunications Law 2004, the provider of publicly available telecommunications services is obligated to apply technical and organisational measures to ensure security and integrity of the network, services and transmission of messages in relation to the services provided and ensuring security of personal data processing (some duties are further specified).

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes, although depending on the type of organisation, the obligation may differ.

Operators of essential services, under the NCS, are required to report information related to Incidents to the appropriate Computer Security Incident Response Team (CSIRT) within 24 hours of the Incident being detected. The obligation is triggered when the operator of essential services classifies the Incident as serious. The notification about the Incident should contain basic information on the Incident, reporting person and entity and measures taken.

Organisations, being digital service providers under the NCS, have similar obligations.

Organisations from the financial sector who provide payment services are also required to report certain Incidents related to payment services and possibly to cybersecurity. Depending on the type of provider, they are required to report to the KNF, or another appropriate authority, operational Incidents, Incidents related to security, Incidents involving an account information service provider (AISP) and a payment initiation service provider (PISP), and provide annual report on frauds related to payment services. The obligation is usually triggered by the sole occurrence of an Incident.

Telecommunications entrepreneurs are required to report to the President of the Electronic Communication Authority (*Prezes Urzędu Komunikacji Elektronicznej*) any breach of security or integrity of the network or services that had a significant effect on the functioning of the network or services, giving information on the breach and any preventive and corrective measures taken. The obligation is triggered by every significant breach.

Moreover, if the Incident has an effect on personal data processed by any organisation, such organisation is required to report such an Incident to the President of the Personal Data Protection Authority (*Prezes Urzędu Ochrony Danych Osobowych*).

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Under the GDPR, when a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. The communication shall describe in clear and plain language the nature of the personal data breach and contain basic information on the Incident specified in the Regulation.

There are situations when communication to the data subject may not be required.

Under the Act on Provision of Electronic Services 2002, the provider is obligated to ensure access by the customer to up-to-date information on special risks related to the use of the electronic service.

Under the Telecommunications Law 2004, when a personal data breach by a provider of publicly available telecommunications services may have adverse effects on the rights of the subscriber or end user who is a natural person, the provider shall immediately notify the breach to the subscriber or the end user with exceptions set out in the Telecommunications Law 2004, e.g. Section 174a, subsect. 5.

The President of the Office of Electronic Communications (UKE) may impose on the telecommunications entrepreneur the obligation to publicly disclose the security or integrity breach of the network or services.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The relevant authorities are:

- President of the Personal Data Protection Office (PUODO) (https://www.uodo.gov.pl).

- Ministers responsible for the relevant sectors – depending on the sector where the given operator of essential services or digital service provider operates, and one central body (Polish Financial Supervision Authority).
- President of the UKE (https://www.uke.gov.pl/).

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Infringements of the provisions concerning personal data connected with cybersecurity issues shall be subject to administrative fines of up to EUR 10 million, or in the case of an undertaking, up to 2% of the total global annual turnover of the preceding financial year, whichever is higher.

Penalties stipulated by the NCS may be up to PLN 200,000; however, if through an inspection of the body responsible for cybersecurity, it is found that the operator of essential services or digital service provider persisted in breaching the NCS, a fine of up to PLN 1 million will be imposed.

The body responsible for cybersecurity may also impose a fine on the managers of the operator of essential services (not exceeding 200% of their monthly salary) if they failed to exercise due care to meet specific obligations.

Penalties imposed by the Telecommunications Law may reach up to 3% of the income of the penalised entity generated in the previous calendar year (imposed both by the President of UKE and the PUODO, as applicable).

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In April 2019, the PUODO issued a PLN 55,750.50 fine to the Lower Silesian Football Association for the unauthorised publishing on the internet of the personal data of people licensed as football referees in 2015. Published data included personal identification numbers and home addresses. It could have been avoided had the Association implemented requirements concerning technical and organisational measures in relation to the IT system used to process personal data.

In March 2019, the PUODO issued a PLN 943,470 fine to a company that failed to provide information on personal data processing (art. 14 of the GDPR) to the entrepreneurs whose personal data the company processed but lacked their email addresses. This could have been avoided had the company implemented requirements concerning technical and organisational measures in relation to the IT system.

In September 2019, the PUODO issued a PLN 2.8 million fine to a company that failed to implement data protection measures adequate to the risks, including: a lack of appropriate response procedures in case of detection of unusual network traffic; and an ineffective system of monitoring potential threats. This could have been avoided had the company implemented requirements concerning technical and organisational measures in relation to the IT system.

In October 2019, the PUODO issued a PLN 40,000 fine to a public entity (city mayor) for violation of the principle of integrity and confidentiality of processing by: storing personal data without a backup system; and failing to conduct a risk analysis. This could have been avoided had the city mayor implemented requirements concerning technical and organisational measures in relation to the IT system.

In November 2019, the PUODO issued a PLN 201,000 fine to a company that failed to implement technical measures, enabling a withdrawal of consent and exercising the right to request deletion of data. This could have been avoided had the company implemented requirements concerning technical and organisational measures in relation to the IT system.

The PUODO issued numerous fines for failure to cooperate with him for the purpose of the proceedings (key obligation in the event of violations related to cybersecurity):

- In March 2020: a fine for preventing an inspection (PLN 20,000).
- In July 2020: a fine for failing to provide the supervisory authority with access to personal data and other information necessary for the performance of its tasks (PLN 15,000).
- In July 2020: a fine for failing to provide the supervisory authority during the conducted inspection with access to premises, data-processing equipment and means, and access to personal data and information necessary for the performance of its tasks (PLN 100,000).
- In February 2021: a fine exceeding PLN 12,000 (EUR 3,000) was imposed on the Warsaw company Smart Cities, for their failure to cooperate with the Polish Data Protection Authority by neither replying to their letter nor providing access to personal data and other information necessary for them to perform their tasks.
- In April 2021: the Polish Data Protection Authority imposed a fine on a television broadcaster, which exceeded PLN 1.1 million (EUR 261,000), as the company failed to implement appropriate technical and organisational measures in its cooperation with the courier company, resulting in numerous breaches being identified with a long delay.
- In June 2021: the Polish Data Protection Authority imposed an administrative fine of PLN 100,000 (EUR 24,000) on company for failing to notify the supervisory authority within 24 hours after having detected a personal data breach.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

Yes. Currently there are no regulations prohibiting the use of beacons. However, due to the fact that beacons may acquire various information, e.g. IP address, which may constitute personal data, all regulations concerning technologies, such as cookies and other similar solutions, apply to beacons.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

Yes. There are no regulations prohibiting the use of honeypots. Moreover, NASK (*Narodowa Akademicka Sieć Komputerowa* – National Academic Computer Network – which is not only a research institute but also one of the three types of CSIRTs) is currently running a research project aimed at early identification and warning about cyberthreats based on honeypots.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Yes. Sinkholes may be used as a measure to detect and deflect Incidents and there are no regulations prohibiting such measures. They are, in fact, used by various organisations (e.g. in the telecommunications sector).

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

1. Recording electronic communications, i.e. data operations in IT systems (their modification, reading, transfer or deletion) and assigning individual actions to specific persons, may constitute, in a specific case, a desirable technical solution to ensure an appropriate (required by law) level of information security.
   Similarly, logging network traffic to/from IT systems often serves as a measure to demonstrate compliance of IT systems with security requirements.
2. In certain cases, however, monitoring or interception of electronic communications may be subject to specific regulations, i.e. the Labour Code (permissible only under some circumstances). Section 222, subsect. 1 of the Labour Code allows this if it is necessary, e.g., for providing employees' safety or property protection. Section 223 of the Labour Code allows for, e.g., monitoring of employees' emails if it is necessary to ensure work organisation, allowing for proper management of full work time and proper usage of working equipment made accessible to the employee. However, while monitoring employees' emails/computers, the employer has to comply with confidence of correspondence and other personal rights of the employee – which includes compliance with the GDPR.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Most governments around the world do not regulate the importation or domestic use of cryptographic features in mass-market products, and the few economies that do typically use a very limited regulatory touch with a narrow product scope.

According to the World Semiconductor Council (WSC) principles for commercial cryptographic technologies in mass-marketed ICT products, the regulation of commercial encryption should be limited and encryption technology mandates should be prohibited, acknowledging the widespread use of encryption and the limited value in regulating the commercial market.

International standardisation in the field of cryptography plays a critical role in enabling both security and interoperability. Many governments around the world acknowledge the benefit of using voluntary global standards instead of regulating encryption in commercial/industrial market ICT products locally.

Nevertheless, pseudonymisation or anonymisation tools must meet specific security requirements resulting in particular from the application of the principles of privacy by design and privacy by default (art. 25 of the GDPR). This means, for example, that anonymisation solutions should not use techniques that are generally considered compromised. Similarly, the pseudonymisation tools must meet a certain level of security with regard to the encryption key management mechanisms. The use of solutions that do not meet the above-mentioned requirements exposes the recipient to liability for non-compliance with information security obligations.

However, in the current legal situation, the status of technology providers (importers/exporters of IT solutions) is not clear. Also, the European Data Protection Board (EDPB) does not explicitly support the acceptance or exclusion of the possibility of controlling technology providers in terms of compliance with art. 25 of the GDPR.

The potential assumption that technology providers are obliged to comply with privacy by design/by default rules opens the way to (for example, showing the relevance of the issue):

- application of art. 84 of the GDPR (introduction of new/use of current national regulations to impose sanctions on the technology provider for violation of art. 25 of the GDPR); and
- assessment of solutions created by the technology provider as 'unlawful' in the event of non-compliance with the requirements of art. 25 of the GDPR (as a result, replacing solutions that are incompatible with such obligations, on the market, could be qualified as a 'unfair competitive practice' and may have all consequences foreseen for such situations, including the obligation to withdraw the solution from the market).

Regardless, importers/exporters of pseudonymisation or anonymisation tools have specific tax and customs obligations.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Market practice varies across different business sectors but there are no recognised deviations from the strict legal requirements. The differences between sectors depend rather on specific characteristics of the sector and the relevance of this sector. Some sectors, e.g. the financial services, telecommunications or new technologies sectors, are naturally more concerned and conscious about information security issues.

Also, under the NCS, public administration became part of the cybersecurity system and fell under further reporting guidelines and procedures, issued by the authorities of adequate level, in regulations other than the Applicable Laws.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Yes, there are specific legal requirements in both sectors.

a. Financial services sector: detailed requirements concerning providing security of information in IT systems for providers of financial services are set out in the Recommendations and Instructions of the KNF and specific statutes. In general, the providers are required to take measures to mitigate risk and develop control mechanisms aimed at risk management and security breach risk management.
b. Telecommunications sector: companies are required (under Section 175, subsect. 1 of the Telecommunications Act) to take technical and organisational measures (providing a level of security appropriate to the risk, regarding the newest

technological achievements and expected costs) aimed at providing security and integrity of the network, services and transfer of messages in relation to the provided services.

See also the answers to questions 2.2. and 2.4.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Managers may be found liable towards the company if an Incident occurs due to their lack of due diligence (i.e. lack of internal procedures required in the given circumstances or failure to enforce them/lack of control if they are applied when they were responsible for compliance matters).

In some cases, a manager may be personally fined under the NCS if, due to his/her negligence, the company that is an operator of an essential service fails to execute regular risk assessments and audits, or fails to make proper notifications of the Incidents.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

a. No; however, under the NCS, companies that are operators of essential services are required to form an internal structure to ensure cybersecurity and designate a contact person to maintain contact with other state cybersecurity system elements.
b. Operators of essential services are required to document cybersecurity measures related to the IT system used to provide essential services. Digital service providers are required to take measures allowing for risk management in relation to cybersecurity, but there is no obligation for a written form. Other companies are not required to establish any written Incident response plan or policy.
c. Operators of essential services are required to conduct periodic cyber risk assessments and management of such risk and perform an audit at least once every two years. Digital service providers are required to take measures allowing for risk management, including monitoring, auditing and testing. Such measures may be necessary, under the GDPR, to any company processing personal data in IT systems – to ensure cybersecurity of such systems – including periodical risk assessment, testing and evaluation of taken technical and organisational measures.
d. Please see the answers above.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Companies rendering electronic services must provide their clients with current information on any particular risks associated with the use of the electronic services provided.

Publicly traded companies must execute their duties on providing the market with current reports and periodic reports, and since cybersecurity risks or Incidents may have a significant effect on their financial or economic situation, they may be required to be disclosed.

The GDPR provides for a procedure on the reporting of Incidents concerning personal data protection (Section 33 of the GDPR).

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The action related to civil liability may be brought against an offender (facing punishment and being liable for damages) or a company that failed to provide proper security measures against an Incident (liable for damages).

Action for damages – under Section 415 of the Polish Civil Code, action can be brought to compensate for actual damage (*damnum emergens*) and cost of opportunity (*lucrum cessans*). Section 444 of the Polish Civil Code allows for the claim damages to cover all costs related to the injury (e.g. medical care and drugs to treat the injury).

Action for compensation – under Section 445 of the Polish Civil Code, in addition to the claim for damages indicated above, the person who suffered injury may also be compensated for any harm suffered (including, e.g. psychological suffering). Section 448 of the Polish Civil Code refers to compensation to cover harm that resulted from the infringement of personal rights (e.g. damage to reputation).

There is also a possibility to bring a civil claim in criminal cases. Under Section 46 of the Polish Criminal Code, if the court convicts the offender, it may order the offender to partially or fully remedy any damage caused by the offence or compensate for any injury. The criminal court applies civil law provisions. This also applies when an offender commits an Incident-related offence (see the answer to question 1.1) and a person suffers damage or injury (e.g. in case the Incident involved a hospital) due to the offence.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

V CSK 141/17 (Supreme Court, 18 January 2018): the bank's client wanted to access her bank account through the internet. She entered her log-in data but was shown a notice saying the website was under maintenance. Later she discovered that the money she had was gone. It was determined in a separate (criminal) proceeding that a third person acquired her log-in data through phishing. The bank was found liable for not providing effective security measures and thus had to compensate for the damage the client suffered.

VI ACa 509/17 (Appeal Court in Warsaw, 30 August 2018): a third person accessed the bank account of a client of a bank and made several transactions for PLN 137,285 in total. The third person used the client's log-in data using the same IP address the client used on the same day. The bank used a two-factor authentication to send several messages (containing verification codes) for the client to authorise the transactions. The client claimed that not all of the used codes were used by him. The client was not sure if his computer was properly secured (e.g. if the software was up to date). The court decided that, in this case,

the client was negligent in taking security measures while using payment services provided by the bank. The court also pointed out that the bank provided effective security measures and could not be held liable for the loss of the client's money.

XXV C 2596/19 (District Court in Warsaw, 6 August 2020): in a judgment, the District Court in Warsaw awarded PLN 1,500 compensation from an insurance company, which provided the injured party with too much information about the policy owner.

Currently, a case is pending against the postal service operator for (in accordance with the lawsuit) obtaining millions of personal data records from the PESEL register and processing them in order to organise presidential elections.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes. Civil liability is based on contract or tort – one does not exclude the other. Liability based on tort includes acts and omissions leading to damage (can be limited in contract), regardless of whether there was a contractual obligation for specific acts or omissions.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. They are permitted and the cybersecurity insurance market is still developing. Taking out insurance against Incidents would also be treated as acting with due diligence while providing technical, organisational and legal measures concerning cybersecurity.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations concerning taking out insurance coverage against any type of Incident. However, insurance can only cover random Incidents – not planned or financed – that cannot be rationally excluded or mitigated.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Various governmental bodies have specific powers. Apart from the police or public prosecutors in criminal proceedings, note that the PUODO, as part of their audit powers, is entitled to access buildings, premises or other spaces, to review documents and information that are directly related to the subject matter of the audit, and carry out inspections of places, objects, equipment, mediums and information systems and ICT systems used to process data.

In accordance with the NCS, a person carrying out inspections of entities that are businesses is entitled to free access to and movement around the premises of the audited entity without the obligation to obtain a security pass to inspect equipment, mediums and information systems.

Similar powers are also held by personnel of the UKE that may also carry out inspections of the audited telecommunications networks and apparatuses.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Yes, under Section 179 of the Telecommunications Act, a telecommunications entrepreneur must take technical and organisational measures of accessing and recording for the police and some other enforcement authorities to access and record telecommunications messages, sent or received by an end user, or terminal telecommunications equipment, and to access and record the metadata of such messages (messages include written, oral and other types of messages).

Under Section 9 of the Counter-terrorism Act of 10 June 2016, the Chief of the Internal Security Agency may order for classified investigative operations concerning an individual who is not a Polish citizen, including obtaining access to and recording data stored on a data storage device or terminal telecommunications equipment, IT systems and ICT systems.

Mateusz Borkiewicz has been advising since 2010 and has advised leaders in the internet industry, particularly in the areas related to GDPR implementation, provision of electronic services, consumer law, cloud computing and intellectual property law.
He has advised on strategic topics concerning, among others, issues of unfair competition, protection of trademarks, cybersecurity, domain disputes, spam, violations of personal rights on the internet (particularly in the context of hate speech towards public figures), managerial bribery and computer crimes, including the theft of virtual currencies.
He has served as Data Security Administrator and Data Protection Officer in several companies operating in the financial services, retail and automotive sectors.
He is the author of two books concerning personal data protection and many professional publications.
He also entered into the list of attorneys kept by the District Bar Council in Wrocław, Poland.

Leśniewski Borkiewicz & Partners (LB&P)
Podwale 83, room 11
50-414 Wrocław
Poland

Tel +48 663 683 888
Email: mb@lbplegal.com
URL: www.lbplegal.com

Grzegorz Leśniewski has been advising since 2009. His main areas of practice include personal data protection, the law of new technologies, cybersecurity and M&A.
Before LB&P Legal, he developed the boutique law firm Leśniewski Legal, under which he advised on, among others, the implementation of GDPR by a Norwegian global provider of telecommunications and cable television services. He has also been the Data Protection Officer at one of the major cloud computing companies in Poland since the entry into force of GDPR.
His former and current clients include, among others, globally present providers of digital products engineering services, multinational telecommunications service providers, the largest Polish social networking site (14 million active users), one of the largest multinational e-commerce businesses in the footwear industry, cloud computing service providers, as well as the market leader of call-centre services in Poland.
He managed the implementation of numerous M&A processes, as well as negotiations in the process of buying/selling companies mostly from the TMT sector.
He also appears on the list of attorneys kept by the District Bar Council in Warsaw, Poland.

Leśniewski Borkiewicz & Partners (LB&P)
Podwale 83, room 11
50-414 Wrocław
Poland

Tel: +48 531 871 707
Email: gl@lbplegal.com
URL: www.lbplegal.com

Jacek Cieśliński has been advising since 2015. His counselling includes ongoing assistance focused largely on areas specific to the new tech sector, such as using modern marketing tools, including behavioural advertising (based on advanced profiling techniques) and remarketing conducted in cooperation with market-leading advertising networks, as well as combining/aggregating databases in groups of companies.
He also advised on the implementation of strategic projects, such as launching mobile applications and advanced stationary biometric scanning technology, combined with an e-commerce account.
He conducted a number of audits in the field of personal data protection and helped raise the awareness of IT/TMT industry employees in order to practically implement data protection standards (trainings for software developers, OPS departments, including second level).
He is associated with leading consulting companies in Poland and the Regional Chamber of Legal Advisers in Wrocław.

Leśniewski Borkiewicz & Partners (LB&P)
Podwale 83, room 11
50-414 Wrocław
Poland

Tel: +48 793 967 934
Email: jc@lbplegal.com
URL: www.lbplegal.com

Leśniewski Borkiewicz & Partners (LB&P) is a modern law firm that works mainly with clients operating within IT, TMT and e-commerce. We know the specifics of the new technologies sector and that allows us to propose practical solutions, taking into account typical risks, market practice and upcoming changes. LB&P has been created as a result of the further development of Leśniewski Legal. It has been formed by people with experience gained in one of the largest Polish advisory companies, as well as in specialised projects realised for international clients.
Our second brand, www.privacyfoxes.com, is dedicated to GDPR issues and implementing solutions for cross-border personal data flows.

www.lbplegal.com

Leśniewski Borkiewicz & Partners

Saudi Arabia


Saeed Algarni


Mohammed Ashbah


Muhanned Alqaidy

Alburhan

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Yes; in accordance with the Anti-Cyber Crime Law ("ACCL"), the penalties vary as per the following four cases:

1. In the case of unlawful access to computers with the intention of threatening or blackmailing any person in order to compel him to take or refrain from taking an action, be it lawful or unlawful: the perpetrator: of this act; unlawfully accessing to a website; or hacking a website with the intention of changing its design, destroying or modifying it, or occupying its URL, shall, according to articles 3-2 and 3-3 of the ACCL, be subject to imprisonment for a period not exceeding one year and a fine not exceeding SAR 500,000, or to either penalty.
2. In the case of illegally accessing bank or credit data, or data pertaining to the ownership of securities in order to obtain data, information, funds or services offered: according to article 2-4 of the ACCL, the perpetrator shall be subject to imprisonment for a period not exceeding three years and a fine not exceeding SAR 2,000,000, or to either penalty.
3. In the case of unlawful access to computers with the intention of deleting, erasing, destroying, leaking, damaging, altering or redistributing private data: according to article 3-5 of the ACCL, the perpetrator shall be subject to imprisonment for a period not exceeding four years and a fine not exceeding SAR 3,000,000, or to either penalty.
4. In the case of unlawful access to a website or an information system directly or through the information network or any computer intending to obtain data jeopardising the internal or external security of the state or its national economy ("CNIs"): according to article 2-7 of the ACCL, the perpetrator shall be subject to imprisonment for a period not exceeding 10 years and a fine not exceeding SAR 5,000,000, or to either penalty.

Denial-of-service attacks
Yes; according to article 3-5 of the ACCL, the perpetrator shall be subject to imprisonment for a period not exceeding four years and a fine not exceeding SAR 3,000,000 or to either penalty.

Phishing
Yes; according to article 1-4 of the ACCL, the perpetrator shall be subject to imprisonment for a period not exceeding three years and a fine not exceeding SAR 2,000,000 or to either penalty.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Yes; according to articles 1-5 and 2-5 of the ACCL, the perpetrator shall be subject to imprisonment for a period not exceeding (four years) and a fine not exceeding SAR 3,000,000 or to either penalty.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Yes, according to article 1-9 of the Arab Convention on Combating Cyber Crime ("ACCC") and the ACCL.

Possession or use of hardware, software or other tools used to commit cybercrime
Yes, according to article 2-9 of the ACCL.

Identity theft or identity fraud (e.g. in connection with access devices)
Yes; according to article 1-4 of the ACCL, the perpetrator shall be subject to imprisonment for a period not exceeding (three years) and a fine not exceeding SAR 2,000,000 or to either penalty.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Saudi law criminalises any attack in any way, and the conviction varies according to the relevant regulations, emphasising that, in accordance with the spirit of Saudi legislation, the criminal penalty for the offender arises because of his or her act of harm, whatever the legal basis.

As for workers, a breach of confidence subjects him to two possible routes of penalty. There is an "internal" path (inside the facility), where, if the worker is still a current employee, the facility shall have the right to either: dismiss him without an end-of-service bonus or compensation for the penalty clause;

or notify him if the accusation is proven against him after the establishment conducted an internal investigation with him and allow him to state his justifications in accordance with article 80 of the Labour Law. In the case of a "foreign" path, where there is a criminal offence, the necessary measures are taken against him, as with any non-worker.

Copyright infringement is condemned in article 21 of the Copyright Law, with five penalties for violations being defined in article 22, as well as the right of the judicial authority to punish defamation (if proven), provided that the penalty does not exceed imprisonment for a period of six months and or the fine is an amount of SAR 250,000, or more than one of the five penalties, and the maximum limits are doubled in case of repetition.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Yes, the perpetrator shall be subject to the same penalty prescribed for the crime itself. However, the penalty may be reduced if the perpetrator submits evidence of good faith to the judiciary based on article 13 of the ACCL.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

1. Yes; according to article 5 of the ACCL, the perpetrator shall be subject to imprisonment for a period not exceeding four years and a fine not exceeding SAR 3,000,000, or to either penalty.
2. If a website, information system or computer device obtains data affecting the national or external security of the state or the national economy, then, according to article 7-2 of the ACCL, the perpetrator shall be punished with imprisonment for a period not exceeding 10 years and a fine not exceeding SAR 5,000,000, or to either penalty.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The Kingdom of Saudi Arabia has jurisdiction over any obligation (negative or positive) that arises, agreed upon or executed inside the Kingdom of Saudi Arabia, and it is exclusively competent with regard to any violations affecting CNIs. The prosecution of criminals under international agreements and bilateral treaties concluded by Saudi Arabia is also a case in point.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Yes; according to article 11 of the ACCL, the court has the right to exempt penalties for an offender who informs the authorities, with three conditions: (1) they must inform them before the damage occurs; (2) they must inform the authorities before they are aware of the Incident in general; and (3) they must inform all other perpetrators, if there are multiple perpetrators.

According to articles 9 and 10 of the ACCL, the penalty does not exceed half of the upper limit if the crime does not occur.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

1. ACCL.
2. Electronic Transaction Law.
3. Telecommunication Act ("TA").
4. Electronic Commerce Law.
5. CITC Ordinance.
6. Criminal Procedure Law.
7. Essential Cybersecurity Controls ("ECC").
8. Critical System Cybersecurity Controls ("CSCC").
9. Copyright Law.
10. ACCC.
11. Rules Governing Insurance Aggregation Activities of Cooperative Insurance Companies Control Law ("RGIAA").
12. The penalties for the dissemination and disclosure of confidential documents and information Act.
13. Cloud Cybersecurity Controls ("CCC").

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Yes, under the Applicable Law, the National Cybersecurity Authority ("NCE") issues controls and standards, and it has issued the first edition of ECC, which must apply to all government agencies, all its subsidiaries, and private sector establishments that own, operate or host CNIs.

The NCE then issued the first version of the CSCC, which is considered a complement to the ECC, except in systems or networks where there has been: disruption or illegal change to the way in which they operate; or unauthorised access to them or to the data and information that they store or process, to the detriment of: the availability of services; the work of the public entity; or the economy, finance or security, or that has a negative social impact at a national level. This was defined in seven precise detailed standards.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the Applicable Law, if the facility owns, operates, or hosts CNIs, it must follow all of the controls issued by the NCE (as per question 2.2), and the controls regarding cooperative insurance establishments are increased according to article 2-5 of the RGIAA. The RGIAA is required to develop a contingency plan that includes the procedures that should be taken in the event of failure of one or more elements of the automated system of the electronic platform. This plan should include corrective measures to ensure the continuity of work and the mechanism of reporting to the establishment.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Saudi Law does not compel facilities to report the attacks, except if the facility owns, hosts or runs CNIs. The Public Prosecution ("PP") is the authority to which it requires information to be reported, according to article 15 of the ACCL. The PP makes its decisions depending on the requirements of each criminal case.

It is worth mentioning that there are many governmental institutions responsible for all aspects of cybersecurity: the Ministry of Communications and Information Technology; the Communications and Information Technology Commission ("CITC"); NCE; the Saudi Data & AI Authority ("SDAIA"); and the Saudi Federation for Cybersecurity, Programming and Drones.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Saudi law does not stipulate that facilities are required to report such information. Unless the establishment has, in its contracts, committed itself under the terms of protection and privacy with customers or suppliers to do so, then it is not exempt from legal liability, except from reporting the Incident, noting that if the authorities request disclosure – in general or in particular – any entity must provide this as such and report accordingly.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

Cases relating to crimes shall be reported to the police, whilst noting that the PP is responsible of investigation, according to article 15 of the ACCL.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Saudi Law does not refer to any such penalties.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

There are no specific examples of this.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There is no legal impediment for the facility to do so, unless it owns, operates or hosts CNIs, in which case it must follow the regulations issued by the NCE.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There is no legal impediment for the facility to do so, unless it owns, operates or hosts CNIs, in which case must follow the regulations issued by NCE.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There is no legal impediment for the facility to do so, unless it owns, operates or hosts CNIs, in which case it must do so following aim 2-5 and its controls in the ECC.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

There is no legal impediment for the facility to do so, unless it owns, operates or hosts CNIs, in which case it must do so following aim 12-2 and its controls in the ECC.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

There is no legal impediment for the facility to do so; the importer must fulfil the detailed requirements of Saudi customs and, if he wants to trade them, obtain the required licences from the Saudi Standards, Metrology and Quality Organization ("SASO"), without prejudice to property rights and other requirements of laws.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Saudi law does not place many restrictions on the movement of the market to its internal organisation, unless the facility wants

to be a listed company, and the market practice differs from one industry to another, as some industries depend on high secrecy protected by written contracts, not the law generally.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

This applies to all government agencies and its subsidiaries, and all establishments that own, operate or host CNIs in accordance with the regulations issued by NCE.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Yes, if the failure of the company clearly relates to the Incident and the company's manager did not take the measures, according to article 32 of the Companies Law, bearing in mind that this is reserved for companies (other than individual institutions) exempt from a large number of obligations. There is no specific law regarding it.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Saudi law does not stipulate that facilities are obligated to do so, except in the following circumstances:

1. With non-individual companies, the responsibility entrusted to the manager increases in achieving all that is necessary for the benefit of the company, including appointing a manager or information and setting a written policy to respond to accidents if this is necessary. Any failure to do so is considered a violation of the law that may lead – if an accident were to happen – to accountability and liability, according to article 32 of the Companies Law.
2. With establishments that own, operate or host CNIs, they must apply the controls issued by the NCE, which made the workforce an integral part of CNIs, and for which the Saudi Framework for Cybersecurity Cadres ("SCyWF") was issued in detail. They are also required to develop a written Incident response policy and to conduct periodic assessments of electronic risks and penetration tests under aim 2 and its controls from the ECC.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There are no specific laws relating to this disclosure. The Companies Law holds the Executive Management responsible for reporting the necessary reports that enable the Board of Directors to know the company's position. The Capital Market Authority ("CMA") also stipulates in its regulations and requirements regarding listed companies the necessity of financial disclosure of risks.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

In respect of the conviction of the perpetrator who caused any violation of cybersecurity, the Criminal Court is the judicial authority responsible for judging the perpetrator with the legally determined penalty against him, and compensation for the damage caused by what he did.

As for the conviction of the company's manager, the judiciary is seeking the help of experts who are assigned the task of investigating and searching for the extent of the failure of the company that took the necessary measures, clearly and without ambiguity, as Saudi law holds managers accountable and it is a case of the principle of trust. Any person who says the opposite will be required to provide such evidence, unless his employment contract or the company's articles of incorporation obligate the manager to take the preventive measures regarding the protection of cybersecurity.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

There are no Incidents that can be disclosed.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

The answer to this question does not differ from the answer discussed to question 6.1, as the harm caused by any person to another makes it legally justified to argue against him, whether it is real or electronic, and whether it is positive or negative (such as negligence).

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Saudi law has no stipulations relating to insurance against Incidents. It is not known if there are companies in this field, and this field may soon be a good legal and investment challenge. It should be noted that the authority concerned with organising all insurance affairs is the Saudi Arabian Monetary Authority ("SAMA").

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no limitations. Insurance companies in Saudi law may exclude or include clauses in their documents, following the approval of the SAMA.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The main relevant authorities are the police, as well as the PP and CITC, according to articles 14 and 15 of the ACCL, under the Applicable Law. In respect of terrorist cybercrime, article 7 of the ACCL stipulates a specific penalty, and the Law on Combating Terrorism Crimes and Financing stipulates that the competent court in terrorism cases is the "Specialised Criminal Court", and many oversights and security agencies work together in fighting terrorism, including the Presidency of State Security in all its sectors.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There is no legal obligation for the facility to do so, unless it owns, operates or hosts CNIs, in which case it must therefore do so under article 56-5 of the TA.

Saeed Algarni is a Managing Partner of Alburhan law firm, specialising in Commercial, Intellectual Property, Data Protection, and Information Technology law. Saeed manages large legal projects for companies and governmental entities and advises on complex commercial matters for a range of local and international clients.

Alburhan
7013 Takhassusi st, Al Rahmaniyah Dist.
RIYADH 12341 – 3507
Saudi Arabia

Tel: +966 555 355 950
Email: saeed@alburhan.sa
URL: www.alburhan.sa

Mohammed Ashbah is a Legal Consultant at Alburhan law firm. Boasting top academic work and nine years' experience working in Riyadh, Ashbah practises Administrative, Franchise, Labour, Cybersecurity Law, and has been recommended as leading in those fields, as well as drafting regulations for regulatory authorities.

Alburhan
7013 Takhassusi st, Al Rahmaniyah Dist.
RIYADH 12341 – 3507
Saudi Arabia

Tel: +966 552 102 207
Email: mhmdashbh@alburhan.sa
URL: www.alburhan.sa

Muhanned Alqaidy practises at Alburhan, focusing primarily on corporate, labour law, regulatory, and administrative law matters. His practice has included a broad and varied representation of public and private corporations and other entities in a variety of industries throughout Saudi Arabia.

Alburhan
7013 Takhassusi st, Al Rahmaniyah Dist.
RIYADH 12341 – 3507
Saudi Arabia

Tel: +966 548 821 310
Email: muhanad@alburhan.sa
URL: www.alburhan.sa

Alburhan is a Saudi law firm that specialises in a broad range of practice areas. It is determined to lead the Middle East region at a time of significant change in the legal industry, by helping clients overcome the challenges of competing in the global economy through a new type of thinking and a different mindset. Alburhan has advised on some of the most complex legal issues, and provides its clients with professional legal expertise, quality strategic advice and maintains a superior level of client service.

www.alburhan.sa

Singapore


Lim Chong Kin


David N. Alfred


Albert Pichlmaier

Drew & Napier LLC

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes. Under section 3(1) of the Computer Misuse Act (Cap. 50A) ("**CMA**"), it is an offence for any person to knowingly cause a computer to perform any function for the purpose of securing access without authority, to any program or data held in any computer. Upon conviction, an offender shall be liable for: a fine of up to $5,000; imprisonment for a term of up to two years; or both for the first offence.

In *Public Prosecutor v Muhammad Nuzaihan bin Kamal Luddin* [1999] 3 SLR(R) 653, the accused was found to have, *inter alia*, exploited certain vulnerabilities to hack into some of the servers of the victim, in order to gain unauthorised access to the computer files contained on the victim's server. The accused was sentenced to two months' imprisonment for the charge under section 3(1) of the CMA.

In *Tan Chye Guan Charles v Public Prosecutor* [2009] 4 SLR(R) 5, the accused was found to have accessed files on a laptop without authorisation, by copying them onto his thumb drive when the laptop's owner left his laptop unattended to answer a phone call. The accused was sentenced to three weeks' imprisonment and fined $5,000.

Denial-of-service attacks

Yes. A denial-of-service ("**DOS**") attack is a cyber-attack meant to shut down a machine or network, thus making it inaccessible to its intended users.

Under section 7(1) of the CMA, any person who, knowingly and without authority or lawful excuse: (a) interferes with, or interrupts or obstructs the lawful use of, a computer; or (b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer, shall be guilty of an offence. Upon conviction, an offender shall be liable for: a fine of up to $10,000; imprisonment for a term of up to three years; or both for the first offence.

There have not been any published judgments by the Singapore courts involving an offence involving a DOS attack.

Phishing

Possibly. Whilst phishing itself may not be an offence, a number of provisions criminalise actions that could include phishing.

Under section 3 of the CMA, it is an offence for any person to cause a computer to perform any function for the purpose of securing access without authority to any data held in any computer. It is possible, depending on the exact circumstances, for this to include phishing. An offender who is convicted under this section shall be liable for: a fine of up to $5,000; imprisonment for a term of up to two years; or both for a first offence.

In *Public Prosecutor v Lim Yi Jie* [2019] SGDC 128, the Court found the accused to have facilitated a phishing scam involving the use of a phishing website, causing a victim to divulge her two-factor-authentication and time-sensitive PIN number to the accused, as the victim assumed that the phishing website was an official bank website. Although the accused was not responsible for the execution of the phishing scam (which, in the Court's view, could be an offence under section 3(1) of the CMA, then named as the Computer Misuse and Cybersecurity Act), the accused had attempted to cash two cheques that were the criminal proceeds of the phishing scam. The accused was thus charged and convicted of an offence under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A).

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes. Under section 5 of the CMA, it is an offence for any person who commits any act that he knows will cause an unauthorised modification of the contents of any computer. As the infection of IT systems with malware would cause an unauthorised modification of the contents of the infected computer, this could be an offence under section 5 of the CMA.

Upon conviction, the offender shall be liable for: a fine of up to $10,000; imprisonment for a term of up to three years; or both for a first offence.

There are presently no published judgments by the Singapore courts involving an offence under the CMA for the infection of IT systems with malware.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

Yes. Under section 8B(1)(b) of the CMA, a person shall be guilty of an offence if that person makes, supplies, offers to supply

or makes available, by any means, any of the following items, intending it to be used to commit or facilitate the commission of an offence under section 3, 4, 5, 6 or 7 of the CMA:

(a) any device, including a computer program, that is primarily designed, adapted, or capable of being used for the purpose of committing an offence under section 3, 4, 5, 6 or 7; and

(b) a password, an access code, or similar data by which the whole or any part of a computer is capable of being accessed.

A person found guilty of this offence shall be liable on conviction for: a fine of up to $10,000; imprisonment for a term of up to three years; or both for a first offence.

There are presently no published judgments by the Singapore courts involving the distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime.

Possession or use of hardware, software or other tools used to commit cybercrime

Yes. Under section 8B(1)(a) of the CMA, it is an offence if a person obtains or retains certain items (as detailed in the following paragraph) and: (i) intends to use it to commit or facilitate the commission of an offence under section 3, 4, 5, 6 or 7 of the CMA; or (ii) does so with a view to it being supplied or made available, by any means, for use in committing or in facilitating the commission of any of those offences.

The items in question are:

(a) any device, including a computer program, that is primarily designed, adapted or is capable of being used for the purpose of committing an offence under section 3, 4, 5, 6 or 7; and

(b) a password, an access code, or similar data by which the whole or any part of a computer is capable of being accessed.

A person found guilty of this offence shall be liable on conviction for: a fine of up to $10,000; imprisonment for a term of up to three years; or both for a first offence.

There are presently no published judgments by the Singapore courts involving the possession or use of hardware, software or other tools used to commit cybercrime.

Identity theft or identity fraud (e.g. in connection with access devices)

Yes. Under section 4 of the CMA, it is an offence for a person to cause a computer to perform any function for the purposes of securing access to any program or data held in any computer, with the intent to commit a number of offences, including certain offences involving fraud or dishonesty. A person convicted of such an offence is liable for: a fine not exceeding $50,000; imprisonment for a term not exceeding 10 years; or both.

Penalties for identity theft and identity fraud are also set out in the Penal Code (Cap. 224) ("**Penal Code**"). Under section 419 read with section 416 of the Penal Code, a person who cheats by personation (i.e., if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is), is guilty of an offence and, upon conviction, liable for: imprisonment for a term of up to five years; a fine; or both. Whilst this offence is of general application, it could also extend to the cyber context.

Separately, section 170 of the Penal Code criminalises the offence of personating a public servant. Any person who is convicted of this offence shall be liable upon conviction for: imprisonment for a term that may extend to two years; a fine; or both.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Yes. Under section 8A(1) of the CMA, it is an offence for a person who, knowing or having reason to believe that any personal information about another person (being an individual) was obtained by an act done in contravention of section 3, 4, 5 or 6 of the CMA:

(a) obtains or retains the personal information; or

(b) supplies, offers to supply, transmits or makes available, by any means the personal information.

Upon conviction, an offender may be sentenced to: a fine of up to $10,000; imprisonment for a term of up to three years; or both for a first offence.

Additionally, it is also an offence under section 136(1) of the Copyright Act (Cap. 63) ("**Copyright Act**") for a person who: (a) makes for sale or hire; (b) sells or lets for hire, or by way of trade offers or exposes for sale or hire; or (c) by way of trade exhibits in public, any article that he knows or ought reasonably to know to be an infringing copy of the work. Upon conviction, an offender may be liable for a fine of up to: $10,000 for the article or for each article in respect of which the offence was committed, or $100,000 (whichever is the lower); imprisonment for a term of up to five years; or both.

In addition, it is also an offence under section 136(3) of the Copyright Act for any person who, at the time when copyright subsists in a work, distributes, for either (a) the purposes of trade, or (b) other purposes (but to such an extent as to affect prejudicially the owner of the copyright), articles that he knows to be infringing copies of the work. Upon conviction, an offender may be liable for: a fine of up to $50,000; imprisonment for a term of up to three years; or both.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Yes. Under section 3(1) of the CMA, any person who knowingly causes a computer to perform any function for the purpose of securing access without authority, to any program or data held in any computer, shall be guilty of an offence. Upon the first conviction, the offender shall be liable for a fine of up to $5,000; imprisonment for a term of up to two years; or both.

Given that penetration testing would necessarily involve gaining access to a computer system, it is possible that such unsolicited penetration testing (i.e., penetration testing done without any authorisation from the owner of the computer system) would constitute an offence under section 3(1) of the CMA.

Even if the penetration testing is unsuccessful, such an act may still be an offence. Under section 10 of the CMA, any person who attempts to commit an offence or does any act preparatory to an offence under the CMA shall be guilty of that offence and shall be liable on conviction for the punishment provided for the offence.

In *Public Prosecutor v James Raj s/o Arokiasamy* [2015] SGDC 36, the accused pleaded guilty and was convicted of the unauthorised hacking of a number of websites, including the websites of a well-known church in Singapore, the blog of a journalist, and a political party's website, as well as the unsolicited scanning and penetration testing of various government servers. The accused was sentenced to six months' imprisonment for the charges pertaining to the unsolicited scanning and penetration testing of various government servers under section 3(1) read with section 10 of the CMA.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Yes. The offences listed under Part II (i.e., sections 3 to 10) of the CMA are generally broad enough to address activities that adversely affect or threaten the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data.

For example, unauthorised modification of computer material (i.e., adversely affecting or threatening the integrity of computer

material) is an offence under section 5 of the CMA, and unauthorised obstruction of use of a computer (i.e., adversely affecting or threatening the availability of a computer system) is an offence under section 7 of the CMA.

Additionally, under section 10 of the CMA, abetments and attempts of the offences under Part II of the CMA are also treated as offences, and a person who abets or attempts to do any act preparatory to or in furtherance of the commission of any offence shall be guilty of that offence.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes, the above offences have extraterritorial application.

In respect of the CMA, section 11 of the CMA provides that the provisions of the CMA shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore. Where an offence is committed outside Singapore, the offender may be dealt with as if the offence had been committed within Singapore, if:

(a) for the offence in question, the accused was in Singapore at the material time;
(b) for the offence in question (being one under section 3, 4, 5, 6, 7 or 8 of the CMA), the computer, program or data was in Singapore at the material time; or
(c) the offence causes, or creates a significant risk of, serious harm in Singapore.

Thus, where a person commits an offence under the CMA from a location outside Singapore, the person in question may nonetheless be prosecuted under the CMA as if the person had committed the offence within Singapore.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Not necessarily. The offences under the CMA do not set out any general exceptions or factors that must be considered by a court in mitigation.

Nonetheless, there are factors that may be taken into account by the court in determining the appropriate sentence. For example, the fact that an offender had no intention to make a financial gain through his actions, and did not, in fact, make any financial gain, may have some impact in mitigating the length of a sentence, or the quantum of a fine.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

There are a number of applicable laws in Singapore relating to cybersecurity. Some of these laws are:

Cybersecurity Act 2018 ("Cybersecurity Act")

The Cybersecurity Act sets out a framework for the monitoring of Critical Information Infrastructures ("**CIIs**"), including imposing obligations on owners of CIIs to report cybersecurity incidents, and provides for the appointment of a Commissioner of Cybersecurity to, amongst others, oversee and promote the cybersecurity of computers and computer systems in Singapore.

In addition, the Commissioner of Cybersecurity is also empowered under the Cybersecurity Act to issue or approve one or more codes of practice of standards of performance for the regulation of owners of CIIs with respect to measures to be taken by them to ensure the cybersecurity of the CII. However, these codes of practice are meant for guidance and do not have legislative effect.

As of the time of writing, the Commissioner of Cybersecurity has issued one such code: the Cybersecurity Code of Practice for Critical Information Infrastructure.

Personal Data Protection Act 2012 ("PDPA")

The PDPA imposes a number of data protection obligations on organisations, in respect of personal data. Importantly, section 24 of the PDPA requires organisations to protect personal data in its possession or under its control by making reasonable security arrangements to prevent: (a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and (b) the loss of any storage medium or device on which personal data is stored.

The PDPA was recently amended by the Personal Data Protection (Amendment) Act 2020 ("**Amendment Act**"), which was passed on 2 November 2020. The amendments introduced by the Amendment Act include two new data protection obligations relating to the data breach notification and data portability. Most of the amendments under the Amendment Act came into force on 1 February 2021, with one notable exception being the provisions relating to data portability (which are presently expected to come into force in early 2022).

Computer Misuse Act (Cap. 50A)

As mentioned above, the CMA covers a number of cyber offences, including, but not limited to, offences such as the exploiting of computer vulnerabilities to gain unauthorised access to a computer system (section 3 of the CMA).

Copyright Act (Cap. 63)

The Copyright Act criminalises copyright infringement. Specifically, it is an offence for a person to, at a time when copyright subsists in a work: (a) make for sale or hire; (b) sell or let for hire, or, by way of trade, offer or expose for sale or hire; or (c) by way of trade, exhibit in public, any article that he knows, or ought reasonably to know, to be an infringing copy of the work.

Strategic Goods (Control) Act (Cap. 300)

The Strategic Goods (Control) Act sets out provisions relating to the transfer and brokering of strategic goods and strategic goods technology. The list of items that have been prescribed by the Minister as strategic goods and strategic goods technology includes "information security" systems, equipment and components (i.e., systems, equipment and components designed or modified to use "cryptography for data confidentiality" having "in excess of 56 bits of symmetric key length, or equivalent").

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The Cybersecurity Act mainly sets out the laws that are applicable specifically to critical infrastructure. Under the Cybersecurity Act, the Commissioner of Cybersecurity may designate a computer or computer system as a CII under the Cybersecurity

Act, if he is satisfied that: (a) the computer or computer system is necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore; and (b) the computer or computer system is located wholly or partly in Singapore.

The list of essential services are set out in the First Schedule to the Cybersecurity Act, which consists of services in the following industries: energy; info-communications; water; healthcare; banking and finance; security and emergency services; aviation; land transport; maritime; services relating to the functioning of Government; and media.

The obligations placed on owners of CIIs include having to report cybersecurity incidents to the Commissioner of Cybersecurity (section 14 of the Cybersecurity Act), conducting regular cybersecurity audits and risk assessments of CII (section 15 of the Cybersecurity Act) and furnishing information on, amongst others, the design, configuration and security of the CII to the Commissioner of Cybersecurity upon the Commissioner of Cybersecurity's written notice to do so (section 10 of the Cybersecurity Act).

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes. Under section 14(2) of the Cybersecurity Act, the owner of a CII must establish mechanisms and processes for the purposes of detecting cybersecurity threats and incidents in respect of the CII, as set out in any applicable code of practice.

Separately, the Protection Obligation under the PDPA requires organisations to put in place reasonable security measures to protect personal data under its possession and/or control. However, the PDPA does not specify the specific measures that organisations should take.

Pursuant to the newly introduced Data Breach Notification Obligation under the PDPA, organisations are required to notify the Personal Data Protection Commission ("**PDPC**") and, in certain cases, the affected individuals, in the event of a data breach that meets certain thresholds. This will be elaborated on in our response to questions 2.4 and 2.5 below.

In its Guide to Managing Data Breaches 2.0 (the "**Data Breach Guide**"), the PDPC sets out what organisations should do to prevent data breaches. First, it states that organisations should implement monitoring measures and tools to provide early detection and warning to organisations. Examples include:

(a) monitoring of inbound and outbound traffic for websites and databases for abnormal network activities;
(b) usage of real-time intrusion detection software designed to detect unauthorised user activities, attacks, and network compromises; and
(c) usage of security cameras for monitoring of internal and external perimeters of secure areas such as data centres and server rooms.

The Data Breach Guide also encourages organisations to put in place a data breach management plan, which would include the following information:

(a) a clear explanation of what constitutes a data breach (both suspected and confirmed);
(b) how to report a data breach internally;
(c) how to respond to a data breach; and
(d) responsibilities of the data breach management team.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes. In respect of data protection, organisations are statutorily required to report Incidents that meet certain thresholds under the Data Breach Notification Obligation of the PDPA. In respect of the Cybersecurity Act, owners of CIIs are statutorily obligated to report Incidents.

PDPA / Amendment Act

Since the PDPA was amended on 1 February 2021, all organisations are required to notify the PDPC in the event of a data breach that meets the statutory thresholds for reporting. These include where the data breach in question: (a) is likely to result in significant harm or impact to the individuals to whom the information relates; or (b) is of a significant scale.

The Personal Data Protection (Notification of Data Breaches) Regulations 2021 ("**DBN Regulations**") specifies the types of personal data that, if the subject of a data breach, are deemed to cause significant harm to the affected individuals. These data include the affected individual's full name or alias or identification number, together with any of the prescribed personal data under the Schedule to the DBN Regulations, such as the salary of the individual. Additionally, the DBN Regulations specifies that a data breach is of significant scale if it affects at least 500 individuals.

Where an organisation has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, section 26C(2) of the PDPA requires the organisation to conduct, in a reasonable and expeditious manner, an assessment of whether the data breach in question is a "notifiable data breach", i.e., whether it meets the statutory thresholds described above. If so, under section 26D(1) of the PDPA, the organisation must notify the PDPC as soon as is practicable of the notifiable data breach, but in any case no later than three calendar days after the day the organisation makes that assessment.

Under regulation 5 of the DBN Regulations, an organisation's data breach notification to the PDPC of a notifiable data breach must be in the form and manner prescribed on the PDPC's website at https://www.pdpc.gov.sg, and must include all of the following information:

(a) the date on which and the circumstances in which the organisation first became aware that the data breach had occurred;
(b) a chronological account of the steps taken by the organisation after the organisation became aware that the data breach had occurred, including the organisation's assessment under section 26C(2) or (3)(b) of the Act that the data breach is a notifiable data breach;
(c) information on how the notifiable data breach occurred;
(d) the number of affected individuals affected by the notifiable data breach;
(e) the personal data or classes of personal data affected by the notifiable data breach;

(f) the potential harm to the affected individuals as a result of the notifiable data breach;
(g) information on any action by the organisation, whether taken before or to be taken after the organisation notifies the Commission of the occurrence of the notifiable data breach, to:
  (i) eliminate or mitigate any potential harm to any affected individual as a result of the notifiable data breach; and
  (ii) address or remedy any failure or shortcoming that the organisation believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach;
(h) information on the organisation's plan (if any) to inform, on or after notifying the Commission of the occurrence of the notifiable data breach, all or any affected individuals or the public that the notifiable data breach has occurred and how an affected individual may eliminate or mitigate any potential harm as a result of the notifiable data breach; and
(i) the business contact information of at least one authorised representative of the organisation.

Additionally, if the organisation does not intend to notify any affected individual affected by a notifiable data breach of the occurrence of that notifiable data breach, the notification must specify the grounds for not notifying the affected individual(s).

The PDPA does not specify that information provided to the PDPC pursuant to a data breach notification will be published. However, persons providing information to the PDPC may identify any such information that is confidential, and provide a written statement giving reasons why the information is confidential (section 59(3) and (4) of the PDPA). In such a situation, the PDPC may nonetheless publish such information (which has been identified as confidential) in the circumstances specified in section 59(5) of the PDPA. These include, *inter alia*, to give effect to any provision of the PDPA or for the purposes of a prosecution.

Cybersecurity Act

Under section 14(1) of the Cybersecurity Act, the owner of a CII must notify the Commissioner of Cybersecurity of the occurrence of any of the following:
(a) a prescribed cybersecurity incident in respect of the critical information infrastructure;
(b) a prescribed cybersecurity incident in respect of any computer or computer system under the owner's control that is interconnected with or that communicates with the critical information infrastructure; and/or
(c) any other type of cybersecurity incident in respect of the critical information infrastructure that the Commissioner has specified by written direction to the owner.

In particular, the owner of the CII is required to notify the Commissioner of Cybersecurity, within two hours after a cybersecurity incident, of the following:
(i) the critical information infrastructure affected;
(ii) the name and contact number of the owner of the critical information infrastructure;
(iii) the nature of the cybersecurity incident, whether it was in respect of the critical information infrastructure or an interconnected computer or computer system, and when and how it occurred;
(iv) the resulting effect that has been observed, including how the critical information infrastructure or any interconnected computer or computer system has been affected; and
(v) the name, designation, organisation and contact number of the individual submitting the notification.

The owner of the CII is then required to provide the following supplementary details within 14 days via the Cyber Security Agency of Singapore's ("**CSA**") website:
(i) the cause of the cybersecurity incident;
(ii) its impact on the critical information infrastructure, or any interconnected computer or computer system; and
(iii) what remedial measures have been taken.

The Cybersecurity Act also generally empowers the Commissioner of Cybersecurity to investigate and prevent cybersecurity incidents (not limited to those involving CIIs), including but not limited to requiring any person to answer any question or to produce any physical or electronic record that is in possession of that person to the incident response officer, which the incident response officer considers to be related to any matter relevant to the investigation.

Under section 43 of the Cybersecurity Act, every person must preserve, and aid in preserving, *inter alia*, all matters relating to a computer or computer system of any person that may have come to the Commissioner of Cybersecurity's and/or incident response officer's knowledge in the performance of his or her functions or the discharge of his or her duties under the Act. For this reason (amongst others), any information furnished would not likely be published.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes, organisations may be required to do so pursuant to the Data Breach Notification Obligation under the PDPA. Under section 26D(2) of the PDPA, on or after notifying the PDPC of a notifiable data breach, the organisation must also notify each affected individual where the data breach in question is likely to result in significant harm to the individual. Notification may be done in any manner that is reasonable in the circumstances.

Notification to the affected individuals is not required or may be prohibited in certain situations specified in the PDPA. Section 26D(5) of the PDPA states that organisations are not required to notify affected individuals if the organisation:
(a) on or after assessing that the data breach is a notifiable data breach, takes any action, in accordance with any prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or
(b) had implemented, prior to the occurrence of the notifiable data breach, any technological measure that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual.

Further, section 26D(6) of the PDPA specifies that an organisation must not notify any affected individual if a prescribed law enforcement agency so instructs or the PDPC so directs.

An organisation may apply to the PDPC for a waiver of the requirement to notify the affected individuals under section 26D(7) of the PDPA.

With respect to the information that must be contained within such a notification to affected individuals, regulation 6 of the DBN Regulations requires such notifications to contain all of the following information:
(a) the circumstances in which the organisation first became aware that the notifiable data breach had occurred;
(b) the personal data or classes of personal data relating to the individual affected by the notifiable data breach;
(c) the potential harm to the affected individual as a result of the notifiable data breach;

(d) information on any action by the organisation, whether taken before or to be taken after the organisation notifies the affected individual:
  (i) to eliminate or mitigate any potential harm to the affected individual as a result of the notifiable data breach; and
  (ii) to address or remedy any failure or shortcoming that the organisation believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach;
(e) the steps that the affected individual may take to eliminate or mitigate any potential harm as a result of the notifiable data breach, including preventing the misuse of the affected individual's personal data affected by the notifiable data breach; and
(f) the business contact information of at least one authorised representative of the organisation.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

There are different regulators responsible for enforcing the above requirements.

The PDPC, which is a division within the Infocomm Media Development Authority ("**IMDA**"), is the regulator responsible for enforcing the provisions under the PDPA.

The Commissioner of Cybersecurity, working together with his team at the CSA, is responsible for the enforcement of the provisions under the Cybersecurity Act.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

There are a range of potential penalties, depending on the exact requirements that have not been complied with.

Under the PDPA, the PDPC is empowered to issue directions to ensure that organisations comply with the PDPA, including imposing a financial penalty of up to $1 million. The Amendment Act will increase the financial penalty that may be imposed to the higher of (a) 10% of an organisation's annual turnover in Singapore, or (b) $1 million. However, this amendment to the maximum financial penalty that may be imposed is not yet in force, and is only expected to come into effect on a date later than 1 February 2022.

Under the Cybersecurity Act, the failure of a CII owner to report a cybersecurity incident in respect of a CII, without reasonable excuse, is an offence and the owner shall be liable on conviction to: a fine of up to $100,000; imprisonment for a term of up to two years; or both.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In respect of non-compliance with the PDPA, the PDPC has published a number of its enforcement decisions.

One of the more notable enforcement cases is *Re Singapore Health Services Pte. Ltd. & Ors.* [2019] SGPDPC 3. In that case, the PDPC took enforcement action against (1) Singapore Health Services Pte. Ltd. ("**SingHealth**"), and (2) Integrated Health information Systems Pte. Ltd. ("**IHiS**"), for failing to put in place reasonable security measures to protect personal data under its possession and control, leading to a data breach wherein the medical records of 1.5 million patients were leaked. The PDPC imposed a financial penalty of $250,000 on SingHealth and $750,000 on IHiS.

There are no published enforcement actions that have been taken against owners of CIIs under the Cybersecurity Act.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

There are likely to be no restrictions on the usage of beacons for protection purposes, *unless* the data collected by such beacons constitutes personal data under the PDPA.

Under the Consent Obligation of the PDPA, organisations are required to obtain consent (or deemed consent) from individuals before the collection, use and disclosure of that individual's personal data. Thus, beacons would not be permissible if they collect personal data without the consent (or deemed consent) of the individuals in question, unless an exception to the Consent Obligation applies under the PDPA.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

There are likely to be no restrictions on the usage of honeypots for the purpose of protection of IT systems. Neither the Cybersecurity Act nor the PDPA restrict the usage of honeypots as a way of protecting IT systems.

In fact, the relevant regulators have addressed the use of honeypots, and do not appear to object to their usage. In an article published by the CSA in 2019, it explained honeypots and their role in cyber defence. Additionally, the PDPC's Guide to Securing Personal Data in Electronic Medium encourages the use of "*defences that may be used to improve the security of networks*".

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)

There are likely to be no restrictions on the usage of sinkholes for the purpose of protection of IT systems. As is the case for honeypots, neither the Cybersecurity Act nor the PDPA restrict the usage of sinkholes for the purpose of protecting IT systems.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Yes, organisations are permitted to monitor or intercept electronic communications on their networks in order to prevent or mitigate the impact of cyber-attacks.

There is no law prohibiting an organisation from monitoring or intercepting electronic communications on their *own* networks. However, if such data falls within the definition of personal data, then the organisation may be required to obtain consent from the relevant individuals.

We note that, under the Protection Obligation of the PDPA, organisations are required to put in place reasonable security measures to protect personal data under its possession or control. Depending on a number of factors, the monitoring or intercepting of electronic communications on an organisation's networks may be considered to be one such reasonable security measure.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Yes. Under the Strategic Goods (Control) Act, the import and export of certain types of strategic goods and strategic goods technology is controlled, including "information security" systems, equipment and components (i.e., systems, equipment and components designed or modified to use "cryptography for data confidentiality" having "in excess of 56 bits of symmetric key length, or equivalent").

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes. The PDPA sets out the baseline standards that all organisations must meet, in respect of the protection of personal data. However, certain sectoral regulators may impose higher standards on a particular industry, especially where the personal data commonly collected, used and disclosed in these industries are sensitive in nature.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Financial Services Sector

In respect of the Financial Services Sector, the Monetary Authority of Singapore ("**MAS**") has set out, in its published Guidelines on Technology Risk Management ("**MAS TRM Guidelines**"), risk management principles and best practice standards to guide financial institutions in: (a) establishing a sound and robust technology risk management framework; (b) strengthening system security, reliability, resiliency, and recoverability; and (c) deploying strong authentication processes to protect customer data, transactions and systems. These include (non-exhaustively) requiring financial institutions to establish a technology risk management framework with oversight by the board and senior management to identify, assess, monitor, report and treat technology risks.

Additionally, the MAS has also issued a Notice on Cyber Hygiene, which requires financial institutions to, amongst others, ensure that security patches are applied to address vulnerabilities in their computer systems, as well as a set of Outsourcing Guidelines, which sets out the MAS' expectations of financial institutions that enter into any outsourcing arrangement or that are planning to outsource its business activities to a service provider.

Healthcare Sector

In the healthcare sector, the Ministry of Health has issued a Cybersecurity Advisory 1/2019 in the wake of the SingHealth data breach in 2018 (*Re Singapore Health Services Pte. Ltd. & Ors.* [2019] SGPDPC 3), which involved the medical personal data of 1.5 million individuals being leaked.

In this Cybersecurity Advisory, all licensees (i.e., hospitals, clinics, etc.) are strongly encouraged to review the Committee of Inquiry's recommendations and cybersecurity best practices, and to implement relevant measures, where appropriate.

Telecommunications Sector

The IMDA has published the Telecommunication Cybersecurity Codes of Practice ("**the Codes**"), which are currently imposed on major Internet Service Providers ("**ISPs**") in Singapore for mandatory compliance. Apart from security incident management requirements, the Codes include requirements to prevent, protect, detect and respond to cybersecurity threats. The Codes were formulated using international standards and best practices, including the ISO/IEC 27011 and IETF Best Current Practices.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Under section 157 of the Companies Act, directors of a company are required to, amongst others, act honestly and use reasonable diligence in the discharge of the duties of their office. In addition, under the common law, directors are also required to carry out their duties with skill, care and diligence.

Thus, if a company fails to prevent, mitigate, manage or respond to an Incident due to a lack of honesty, or a lack of the requisite skill, care and diligence on the part of its directors, this may constitute a breach of directors' duties.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

(a) There is no present requirement for companies to designate a CISO under the relevant cybersecurity laws. The provisions of the Cybersecurity Act generally apply to owners of CIIs.

In respect of the PDPA, companies are required to appoint a Data Protection Officer ("**DPO**") under section 11(3) of the PDPA, whose duties include, amongst others, to:

- ensure compliance of PDPA when developing and implementing policies and processes for handling personal data;
- foster a data protection culture among employees and communicate data protection policies to stakeholders;
- manage data protection-related queries and complaints;
- alert management to any risks that might arise with regard to personal data; and
- liaise with the PDPC on data protection matters, if necessary.

(b) Under the Cybersecurity Act and the Cybersecurity Code of Practice for Critical Information Infrastructure, owners of a CII may be required to establish a written Incident response plan or policy in respect of that CII.

In respect of the PDPA, there is no specific requirement to establish a written Incident response plan or policy.

However, section 12 of the PDPA requires organisations to, amongst others, develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA. This would likely include developing a policy relating to the handling of security incidents and data breaches.

In respect of the above, the PDPC has recommended in its Data Breach Guide that organisations put in place a data breach management plan, which should set out, amongst others, how the organisation should respond to a data breach.

(c) Under the Cybersecurity Act and the Cybersecurity Code of Practice for Critical Information Infrastructure, owners of a CII may be required to conduct periodic cyber risk assessments.

There is no specific requirement under the PDPA for companies to conduct periodic cyber risk assessments, including for third-party vendors. However, in its Advisory Guidelines on Key Concepts in the PDPA, the PDPC has stated that organisations should take steps to ensure, amongst others, that its computer networks are secure, and that its IT service providers are able to provide the requisite standard of IT security.

(d) Under the Cybersecurity Act and the Cybersecurity Code of Practice for Critical Information Infrastructure, owners of a CII may be required to conduct periodic cyber risk assessments, which may include penetration testing and vulnerability assessments.

There is no specific requirement for companies to perform penetration tests or vulnerability assessments under the PDPA. However, as above, the PDPC has stated in its Guide to Data Protection Impact Assessments that organisations may conduct penetration tests as part of their reasonable security arrangements to protect personal data. We further highlight that certain sectoral regulators in Singapore impose more stringent requirements on organisations within that sector. For example, the MAS imposes certain requirements in respect of cybersecurity on its licensees, including requiring its licensees to implement robust security measures to ensure that their systems and customer data are well protected against any breach or loss.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

No, companies are not subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents, other than those already mentioned above (i.e., to the relevant regulatory bodies).

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

If an Incident gives rise to a private actionable claim, the affected individual may have recourse against the organisation that caused the Incident.

Section 48O of the PDPA (which replaced the previous section 32 of the PDPA when the PDPA was amended by the Amendment Act) provides for a right of private action. Under this section, any person who suffers loss or damage directly as a result of a contravention of the organisation's obligations under Parts IV, V, VI, or VIA of the PDPA (which set out organisations' obligations to protect individuals' personal data) shall have a right of action for relief in civil proceedings in a court. This includes a breach of section 24 of the PDPA, which requires organisations to protect personal data that is in its possession or under its control (as outlined further above).

Under the CMA, a court may order an offender to pay a compensation amount to a victim of the offence. The victim may also pursue a civil remedy against the offender separately, as the order for payment of compensation does not prejudice the right of the victim to recover more than was compensated to him under the compensation order.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

In *IP Investment Management Pte Ltd and others v Alex Bellingham* [2019] SGDC 207, the third plaintiff (a natural person) successfully obtained an order enjoining the defendant, a former employee of the first and second plaintiffs (which were corporate entities engaged in a fund management business), from using, disclosing or communicating his personal data, and also obtained an order for the defendant to deliver up any copies of his personal data.

Finding the case in favour of the third plaintiff, the court held that the defendant had breached his obligations under the PDPA; in particular, the Consent Obligation and Purpose Limitation Obligation. The court also found that the third plaintiff had suffered loss as a result of the defendant's breach of the Consent Obligation and Purpose Limitation Obligation.

It is worth noting that the court found that the first and second plaintiffs had no legal standing to bring the claim under the then section 32 of the PDPA (before the PDPA was amended under the Amendment Act), as it held that the then section 32 of the PDPA did not extend to corporate entities. Thus, as the first and second plaintiffs were corporate entities, their applications were disallowed by the court.

On appeal, the High Court found that the third plaintiff did not have a right of private action under the then section 32 of the PDPA, because he had not suffered any loss or damage within the meaning of the provision. The appeal was allowed and the order made by the state court was set aside.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes. Depending on the circumstances of the Incident, it is possible that one or more causes of action in tort may be applicable. For example, if an organisation had breached its duty of care under the tort of negligence, by failing to put in place measures to prevent an Incident, the organisation may be found liable under this tort.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents in Singapore.

As of the date of writing, a number of insurance providers in Singapore provide cyber insurance, which covers, amongst others, data protection/personal data liability and corporate data liability.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are presently no regulatory limitations to insurance coverage against specific types of loss in respect of cyber insurance.

However, it bears noting that as insurance contracts are ultimately contracts, they are also subject to contractual law principles. These principles include, amongst others, that such a contract will be enforceable only if it is not tainted by illegality or is contrary to public policy.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

There are a number of laws that would provide investigatory powers to the relevant regulators/law enforcement personnel.

Generally, the Singapore law enforcement authorities have fairly broad powers under the Criminal Procedure Code (Cap. 68) ("**CPC**") to access, inspect and check the operation of any computer that they suspect is or has been used in connection with, or contains or contained evidence relating to, an arrestable offence. This may include offences under the CMA.

In relation to the PDPA, section 50 of the PDPA empowers the PDPC with powers of investigation to investigate whether organisations are in compliance with the PDPA. The powers are set out in the Ninth Schedule of the PDPA, which includes, amongst others, the power to require documents or information to be produced by the organisation to the PDPC, as well as the power to enter premises (both without and with a warrant), subject to certain conditions being satisfied.

In relation to the Cybersecurity Act, the Commissioner of Cybersecurity is empowered under sections 19 and 20 to investigate and prevent cybersecurity incidents. These powers include requiring, by written notice, any person to produce to the incident response officer appointed by the Commissioner of Cybersecurity, any physical or electronic record, or document that is in the possession of that person.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No, there are no requirements for organisations to implement backdoors in their IT systems for law enforcement authorities. However, there is a requirement (under certain circumstances) to provide law enforcement authorities with encryption keys.

Under section 40 of the CPC, for the purposes of investigating an arrestable offence, an authorised police officer or other authorised person can require any person whom he reasonably suspects to be in possession of any decryption information, to grant him access to such decryption information as may be necessary to decrypt any data required for the purposes of investigating the arrestable offence.

Lim Chong Kin heads Drew & Napier LLC's Technology, Media and Telecommunications Practice Group, and is co-head of the firm's Data Protection, Privacy & Cybersecurity Practice.
Under Chong Kin's leadership, these practices are consistently ranked as the leading practices in Singapore. His clients include the telecoms and media regulators, global carriers, technology market leaders, global broadcasters and content providers.
Chong Kin has been an external legal and regulatory advisor for the PDPC of Singapore since 2013, and he played a key role in the liberalisation of Singapore's telecoms, media and postal sectors, where he drafted the competition frameworks.
Chong Kin is highly regarded by his peers, clients and rivals alike for his expertise, and is consistently recommended as a leading lawyer by major international legal publications such as *Chambers Asia-Pacific*, *The Legal 500 Asia Pacific*, *Who's Who Legal*, *The Guide to the World's Leading Competition & Antitrust Lawyers/Economists*, *Global Competition Review*, *Practical Law Company – Which Lawyer?*, *Asialaw Profiles* and *Best Lawyers*.

Drew & Napier LLC
10 Collyer Quay
10th Floor, Ocean Financial Centre
Singapore 049315

Tel: +65 6531 4110
Email: chongkin.lim@drewnapier.com
URL: www.drewnapier.com

David N. Alfred is a director of Drew & Napier LLC and co-head of the firm's Data Protection, Privacy & Cybersecurity Practice. He is concurrently co-head and programme director of the Drew Data Protection & Cybersecurity Academy. David is a data protection, cybersecurity and technology lawyer with over 20 years' experience advising on a broad range of matters relating to digital technology, telecommunications and the Internet.
David's practice over the last 10 years has focused on data protection and cybersecurity. He has substantial experience advising on data protection compliance, public policy and legislation, regulatory enforcement, data breaches and international aspects of data protection.
Prior to joining the firm, David was the first Chief Counsel to Singapore's data protection authority, the PDPC. He has also worked in other in-house roles, including with Singapore's media and telecom regulator, the IMDA.

Drew & Napier LLC
10 Collyer Quay
10th Floor, Ocean Financial Centre
Singapore 049315

Tel: +65 6531 2342
Fax: +65 6535 4864
Email: david.alfred@drewnapier.com
URL: www.drewnapier.com

Albert Pichlmaier is a senior cybersecurity engineer with Drew & Napier LLC and concurrently course director (cybersecurity) with the Drew Data Protection & Cybersecurity Academy. Albert is an IT professional with 30 years of international experience in the private and public sectors. He has worked in a wide range of IT and security domains, from smart card firmware development and test automation, to artificial intelligence and blockchain development. Albert holds a degree in computer science and the CISSP and CDPSE certifications.
Prior to joining the firm, Albert worked for over 10 years in the public sector in Singapore. Most recently, he worked with Singapore's data protection authority, the PDPC, where he was involved in technology and cybersecurity assessments for data protection compliance and enforcement cases. Prior to that, he was the technical manager for common criteria certifications with the Info-communications Development Authority of Singapore.

Drew & Napier LLC
10 Collyer Quay
10th Floor, Ocean Financial Centre
Singapore 049315

Tel: +65 6531 4108
Fax: +65 6535 4864
Email: albert.pichlmaier@drewnapier.com
URL: www.drewnapier.com

Drew & Napier LLC has provided exceptional legal advice and representation to discerning clients since 1889 and is one of the leading and largest law firms in Singapore.
The firm's work in data protection, privacy and cybersecurity precedes the advent of Singapore's Personal Data Protection Act 2012 and Cybersecurity Act 2018. Over the last decade, Drew & Napier has been one of the leading Singapore practices in the fields of data protection, privacy and cybersecurity. The firm has advised and acted for a wide range of clients on a variety of matters that run the full gamut. These include the implementation of group-wide data protection compliance programmes, localisation of global data privacy policies, data protection training programmes, requirements of Singapore's Cybersecurity Act 2018, developing a data breach management plan, dealing with data breaches and cybersecurity incidents (whether involving hacking, malware or accidental disclosure), data breach reporting requirements, conducting data protection and regulatory risk audits and addressing *ad hoc* legal queries.

www.drewnapier.com

DREW & NAPIER

Sweden


Jonas Forzelius


Esa Kymäläinen

TIME DANOWSKY Advokatbyrå AB

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking is considered a breach of data security (Sw: *dataintrång*) under the Swedish Criminal Code and is punishable either by a fine or imprisonment for up to two years. Serious offences are punishable by imprisonment for at least six months and up to six years.

If a breach of data security, such as hacking, is committed by an employee of a company, it may result in an administrative penalty for the company, if the company is deemed not to have implemented sufficient measures to prevent breaches of data security or if the offender holds a leading position or similar in the company. This also applies to foreign companies conducting business activities in Sweden.

In 2014, a police officer was convicted by the Swedish Supreme Court for breach of data security after having used the internal IT system at the Swedish Police Authority to carry out searches for private purposes. The officer in question had solicited access to the system for professional purposes only and was therefore sentenced to a fine for the unauthorised searches.

Denial-of-service attacks
To prevent or seriously disturb the use of electronic information is considered a breach of data security under the Swedish Criminal Code and, consequently, punishable by a fine or imprisonment for up to two years. Serious offences are punishable by imprisonment for at least six months and up to six years. A breach of data security may also entail corporate fines if the offence is committed by an employee of a company.

Phishing
Phishing is considered fraud (Sw: *bedrägeri*) under the Swedish Criminal Code and is punishable by a fine or imprisonment for up to two years. Serious offences are punishable by imprisonment for at least six months and up to six years.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
The Swedish Court of Appeal has ruled that unauthorised installation of software on a computer is not considered a breach of data security itself. If, however, the installation constitutes an intentional alteration, deletion or blocking of electronic information in the system, the prerequisites for breach of data security are met.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
The distribution, sale or offering for sale of products used to commit a breach of data security may constitute complicity or preparation to commit a breach of data security, which is considered a crime under the Swedish Criminal Code. Preparation to commit a breach of data security is punishable by a fine or imprisonment for up to two years. Serious offences are punishable by imprisonment for at least six months and up to six years. The same applies for complicity.

Possession or use of hardware, software or other tools used to commit cybercrime
The possession or use of tools to commit a breach of data security does not itself constitute a crime but may amount to complicity or preparation to commit a breach of data security, which is considered a crime under the Swedish Criminal Code. Preparation to commit a breach of data security is punishable by a fine or imprisonment for up to two years. Serious offences are punishable by imprisonment for at least six months and up to six years. The same applies for complicity.

Further, the use, development, marketing or possession of technical instruments, components or services with the purpose of gaining unauthorised access to copyright protected materials may constitute a breach of the Swedish Copyright Act, punishable by a fine or imprisonment for up to two years.

As for hardware or software designed to be used for decoding of certain services, as defined in the Swedish Act on Decoding (e.g. radio and TV broadcasting), the development, marketing or possession of such tools may constitute a breach of said act and is punishable by a fine or imprisonment for up to two years.

Identity theft or identity fraud (e.g. in connection with access devices)
Identity theft and identity fraud is criminalised as unlawful identity use (Sw: *olovlig identitetsanvändning*) under the Swedish Criminal Code and punishable by a fine or imprisonment for up to two years.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Copyright infringement (Sw: *upphovsrättsbrott*) is subject to the penal provisions pursuant to the Swedish Copyright Act and punishable by a fine or imprisonment for up to two years.

In general, disclosing information subject to an employer-employee confidentiality agreement does not, itself, constitute a breach of law. However, subject to the Swedish Trade Secrets Act (Sw: *Lag om företagshemligheter*), the disclosure of information defined as trade secrets may amount to a criminal offence,

punishable by a fine or imprisonment for up to two years. Serious offences are punishable by imprisonment for at least six months and up to six years.

Further, as regards professions that are subject to statutory confidentiality, e.g. for doctors, breaches of confidentiality ("breach of duty of confidentiality", Sw: *brott mot tystnadsplikt*) are punishable under the Swedish Criminal Code by a fine or imprisonment for up to one year.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Penetration testing is a commonly used method amongst organisations to secure and develop IT systems in order to comply with cybersecurity regulations. However, unsolicited penetration testing may constitute and be punishable as a breach of data security under the Swedish Criminal Code, which is applicable to breaches of any form of data within an IT system regardless of any intention to make use of or damage it.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

In addition to the abovesaid, it may be noted that an action causing damage to physical equipment, such as computers, servers, etc. may constitute an act of damage to property (Sw: *skadegörelse*), which is punishable under the Swedish Criminal Code by imprisonment for up to two years.

Damaging or destroying certain equipment of considerable importance in providing defence, supplying the needs of the population, the administration of justice or public administration in the country, or the maintenance of public order and security in the country, may constitute sabotage (Sw: *sabotage*), which is criminalised under the Swedish Criminal Code and punishable by a fine or imprisonment for up to two years. Serious offences are punishable by imprisonment for at least six months and up to six years.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Generally, extraterritorial application of the Swedish Criminal Code requires that the relevant offence is also criminalised in the country where it was committed. Additionally, extraterritorial application presupposes a certain connection to Sweden as defined in the Swedish Criminal Code, e.g. that the offence has been committed by a Swedish citizen or a foreigner residing in Sweden, or that the offence is punishable by more than six months' imprisonment and has been committed by a foreigner residing abroad but currently located in Sweden.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Most of the above-mentioned offences are criminalised as breach of data security under the Swedish Criminal Code, through which the requirements of EU law have been implemented. Criminal liability under said provision applies to different forms of unauthorised, intentional disposals of electronic information, such as hacking, denial-of-service attacks, phishing, infections of IT systems, etc. Accordingly, unintentional acts are not considered criminal breaches of data security. Criminal liability is also exempted in cases of authorised or consented access, such as assignments to perform penetration tests. However, this exception does not necessarily apply to acts without intent to cause damage and/or make a financial gain; the mere unauthorised access or disposal of electronic information constitutes a breach of data security.

Liability for complicity and preparation to commit offences under the Criminal Code, such as breach of data security, may be exempted in certain cases. The use, possession, distribution or sale of tools used to commit cybercrime does not entail criminal liability for preparation, if the tools in question lack clear connection to the criminal activity. Voluntary resignation may also exempt liability for preparation. There is no exception applicable for completed offences, but the penalty may be mitigated if the offender tried to prevent the offence or reduce the damage caused by it.

Unlawful disclosures under the Swedish Trade Secret Acts may, under certain circumstances, be deemed lawful. An employee, for instance, may disclose trade secrets to the public or the authorities if the disclosure aims to reveal something that can reasonably be suspected to constitute a crime that may lead to imprisonment, or if the information otherwise reveals misconduct deemed to be of public interest.

There are also some general exceptions for criminal copyright infringements under the Swedish Copyright Act (e.g. private use, educational purposes, etc.).

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Cybersecurity legislation extends over several areas of Swedish law:

- Data protection, particularly the processing of personal data, is regulated directly by the EU General Data Protection Regulation (GDPR).
- Personal data-processing by governmental authorities responsible for crime prevention, investigation and prosecution is regulated by the Swedish Act on Processing of Personal Data Relating to Criminal Offences (Sw: *Brottsdatalagen*).
- Criminal offences, including cybercrimes such as breaches of data security, are subject to the Swedish Criminal Code (Sw: *Brottsbalken*).
- Copyright infringement is regulated by the Swedish Copyright Act (Sw: *Lag om upphovsrätt till litterära och konstnärliga verk*).
- Decoding activities regarding radio and TV are criminalised and regulated by the Swedish Act on Decoding (Sw: *Lagen om förbud beträffande viss avkodningsutrustning*).
- Acts of terrorism, including cyber-attacks, are regulated by the Swedish Act on Criminal Responsibility for Terrorist Offences (Sw: *Lag om straff för terroristbrott*).
- Providers of electronic communication services are subject to the Swedish Act on Electronic Communication (Sw: *Lag om elektronisk kommunikation*).
- Certain entities that providing critical infrastructure services or IT systems are subject to the EU Directive

on Security of Network and Information Systems (NIS), which has been implemented by the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services (Sw: *Lag om informationssäkerhet för samhällsviktiga och digitala tjänster*).

- The Swedish Act on Payment Services regulates payment services provided in Sweden (Sw: *Lag om betaltjänster*).
- Disclosure of trade secrets is prohibited by the Swedish Trade Secrets Act (Sw: *Lag om företagshemligheter*).

Further, certain operations and activities deemed important to Swedish national security are regulated by the Swedish Protective Security Act (Sw: *Säkerhetsskyddslag*).

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The Swedish Protective Security Act and the Protective Security Ordinance requires security-sensitive entities and businesses to prevent information security Incidents and damages and to classify security-sensitive data.

Furthermore, in light of the development of 5G, a new EU directive will be implemented to Swedish law by amending the Swedish Act on Electronic Communications. The directive aims to ensure that the usage of radio transmitters will not constitute a threat to Swedish national security but also entails new obligations towards customers.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The GDPR regulates data controllers and processors processing personal data, the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services regulates providers of critical infrastructure services, the Swedish Act on Electronic Communications regulates electronic service providers and the Swedish Act on Payment Services regulates providers of payment services. These acts contain obligations for organisations to implement appropriate technical and organisational measures, generally including monitoring, detecting, preventing, and mitigating Incidents.

Organisations carrying out security-sensitive activities are also obligated to establish and document security needs, plan and enforce security measures (such as classifying data), and follow up on the security work of the organisation. Such organisations must also report any important information to the relevant supervisory authority.

The Swedish Civil Contingencies Agency has issued regulations and requirements that all governmental authorities must follow. This includes drafting security policies and documenting security measures taken.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Several laws require organisations to report Incidents to different authorities. The extent to which Incident-related information must be reported, however, is generally not explicitly regulated by law but instead depends on the nature of the individual Incident.

The GDPR requires data controllers to report personal data Incidents to the Swedish Authority for Privacy Protection without undue delay and not later than 72 hours after having become aware of it, unless the Incident is of minor importance. The report should describe the nature of the Incident, such as the scope of individuals and the categories of data subjects affected. Furthermore, the likely effects of the data breach, as well as a description of measures taken or proposed to address such effects, must be reported. The data controller must also provide its contact details to the authority.

Banks, health services and other providers of critical infrastructure services must report Incidents to the Swedish Civil Contingencies Agency without undue delay. This follows from the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services. The supervisory authority drafts regulations specifying the information that such a report should include.

Any organisation that conducts security-sensitive activities under the Swedish Protective Security Act is required to report Incidents to the supervisory authority, which may be either the Swedish Security Service or the Swedish Armed Forces.

Severe interruptions in electronic services must be reported by the provider to the Swedish Post and Telecom Authority. An Incident is defined as an unlawful destruction, disclosure, or access to information. The provider must notify the authority within 24 hours in case of an integrity Incident. If any subscribers to the electronic service are affected by the Incident, the provider is obliged to notify them as well.

Providers of payment services subject to the Swedish Act on Payment Services are obliged to report Incidents to the Swedish Financial Supervisory Authority without undue delay. The providers must also notify any affected individuals and provide them with information about the Incident and how to mitigate the effects of it.

Generally, all individuals have the right to request and access documents from governmental authorities. This follows from the Principle of Public Access to Official Records. However, exceptions can be made if the requested information can be considered confidential.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The GDPR requires data controllers to communicate any personal data Incident that is likely to result in a high risk to the rights of the affected data subject.

Entities subject to the Swedish Act on Electronic Communications are required to report Incidents to affected subscribers without undue delay. The same applies to providers of payment services under the Swedish Act on Payment Services whenever an Incident entails risks to user transactions.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The Swedish Post and Telecom Authority is responsible for supervising compliance of the Swedish Act on Electronic Communications. The Swedish Authority for Privacy Protection is responsible for GDPR-related issues. Supervision of matters related to the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services are shared between the Swedish Post and Telecom Authority and the Swedish Civil Contingencies Agency. The latter is responsible for handling Incident reports, among other things, while the Swedish Post and Telecom Authority is responsible for the supervision of the digital sector, i.e. cloud services.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Failure to comply with the GDPR, including its requirements on Incident reports and/or the implementation of technical and organisational measures, may result in an administrative fine. The amount payable depends on the extent and gravity of the infringement. It may, at most, amount to the highest of 20 million euros or four per cent of the data controller's worldwide annual turnover. Actors within the public sector may be fined up to 5 million SEK for less serious infringements and up to 10 million SEK for more serious infringements.

Infringements of obligations under the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services may result in a fine between 5,000 SEK and 10 million SEK. The same applies to failure to comply with the Swedish Act on Payment Services, where, however, the maximum amount payable is set to 50 million SEK.

Non-compliance with the Swedish Act on Electronic Communications may result in a fine or up to six months' imprisonment.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Since the Swedish Authority for Privacy Protection started investigating GDPR compliance in June 2018, several penalties, such as warnings, injunctions and administrative fines, have been issued towards non-compliant organisations. One high-profile case is the Authority for Privacy Protection's decision from March 2020 to impose a 75 million SEK fine on Google for failure to comply with the GDPR. According to the authority, Google had not fulfilled its obligations in respect of the right to request delisting from the search engine. Subsequently, the authority´s decision to impose an administrative fine was tried and was reduced to 52 million SEK by the Stockholm Administrative Court (in the judgment of 23 November 2020). Both parties have appealed against the judgment and the case is pending (September 2021) in the Administrative Court of Appeal.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
According to the Swedish Act on Electronic Communication, as well as the GDPR, the use of web beacons is permitted.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There are no explicit provisions in Swedish law to address honeypots. However, the honeypot mechanism may in some specific cases be considered a sting operation, which is prohibited as a law enforcement method in Sweden.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
The use of sinkholes is not prohibited where consent is provided by the relevant operator; however, such use may result in legal difficulties depending on the nature of the information that is received and re-directed.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Yes, if it is considered necessary and justified and the employee has been informed that such monitoring may occur. Due to the unbalanced relationship between an employer and employee, however, the employee may not be considered able to freely consent to monitoring and network interception. The employer must ensure that such supervisory measures are compliant with applicable laws. For instance, if the monitoring includes processing of the employee's personal data, the GDPR must be considered.

Further, employees are bound to fulfil a general duty of loyalty towards their employers. This duty may include an obligation to report cyber Incidents.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Export restrictions may apply for technology designed to prevent or mitigate the impact of cyber-attacks. EU law and Swedish legislation regulate the control of dual-use products, i.e. products with established civilian functions that can also be used for military purposes. EU Regulation 2019/2199 establishes a list of restricted dual-use items, including telecommunications and "information security" items. Control and compliance are handled by the Swedish Inspectorate for Strategic Products.

Some cryptographic equipment is included in the list of export-restricted dual-use items, but not for private use.

The above-mentioned regulation does not restrict transit within the EU or import.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Some market practices deviate from legal requirements through application of general standards implemented to ensure and simplify regulatory compliance. Examples of such standards are ISO 27002:2018, ISO 27001:2017 and NIST 800-88, none of which are mandatory. It is complicated to shortly detail business sectors subject to different standards; however, the financial and telecom sectors are generally more regulated than other sectors.

The Swedish Financial Supervisory Authority issues non-mandatory recommendations and regulations and regularly investigates compliance and standards. Also, the Swedish Standards Institute (SSI) provides standards to member companies, organisations and agencies and adopts European standards as part of the European Committee for Standardisation.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

As mentioned in section 2, several laws apply to entities in different sectors in relation to cybersecurity. The legal requirements vary depending on the type of activity that they carry out.

Actors in the financial sector, such as banks, are bound to comply with certain regulations and guidelines issued by the Swedish Financial Supervisory Authority with regard to their IT systems.

The Swedish Act on Electronic Communications, which regulates electronic service providers, and the Swedish Act on Payment Services, which regulates providers of payment services, both contain obligations on providers to implement the appropriate technical and organisational measures, and general include monitoring, detecting, preventing, and mitigating Incidents.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Directors and officers are not personally responsible for breaches of Applicable Law by the company. However, if the company is penalised due to the directors' failure to take appropriate measures to comply with Applicable Laws, the director may be subject to sanctions in accordance with Swedish labour law.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

a) There are currently, in most cases, no requirements under any Applicable Laws to designate a Chief Information Security Officer (CISO). In some cases, the GDPR demands that a Data Protection Officer (DPO) be appointed, e.g. for public authorities or bodies. Further, the GDPR, the Swedish Protective Act, the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services and the Swedish Act on Electronic Communications all require certain technical and organisational measures. However, technical and organisational measures are not defined in detail. The Swedish Act on Electronic Communications is expected to be updated at the turn of the year 2021/2022, due to the European Electronic Communications Codex (EECC) Directive. The EECC directive brings some clarification, e.g. by providing a definition of "security measures".

b) If a company is affected by the Swedish Protective Security Act, it must ensure that a Protective Security Officer is appointed, which could be considered equivalent to a CISO.

c) As for the GDPR, a written Incident response plan should be adopted to ensure that all requirements of the GDPR are fulfilled when dealing with a personal data breach, e.g. in order to comply with the maximum 72-hour reporting period.

d) Companies subject to the Swedish Protective Security Act are required to carry out protective security analyses and adopt protective security measures. It is not explicitly stated whether they need to be periodic or not, but the analyses must be updated when needed.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Companies that are listed on the public market are required by the Swedish Act on Market Abuse to disclose information that may affect the market price of the shares to the public. The obligation to make such information public applies without regard to the origin of the information, albeit with some exceptions.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The GDPR provides data subjects with different rights, *i.a.*, the right to be forgotten and, in certain situations, the right to consent before personal data is transferred to a third party. If such rights are ignored by a processing entity, the data subjects may file a lawsuit against the processing entity, which may result in a right to damages for the data subject.

A civil action may be brought on many different grounds. In case of an Incident, there are generally several ways to seek damages inflicted from the responsible party.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

In 2015, the Court of Appeal afforded damages of a total value of 5,000 SEK to be paid by a data intruder to the plaintiff. The case was brought by a public prosecutor against the data intruder, whereas the damages were sought by the plaintiff.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

The Swedish Tort Liability Act provides a general possibility to seek remedies for damages caused by, e.g. negligence. However, The Swedish Tort Liability Act is subsidiary to other legislation, such as the GDPR.

Article 82 of the GDPR grants any physical person, who has suffered material or non-material damage a result of an infringement of the Regulation, the possibility to seek compensation from the responsible data controller or processor.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

In general, it is possible for organisations to purchase insurance against third-party claims, e.g. due to a data breach. However, it is unlikely for a person to be able to insure himself against claims from authorities, or for liability due to their own criminal actions, e.g. as breaches of data security, albeit this is not totally clear in Sweden.

An affected party, on the other hand, is entitled to insurance compensation even if the damage was caused by a criminal action.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no limitations as to types of loss an insurance may cover, with the exception of administrative fines and sanctions imposed by the authorities.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The authorities differ depending on the sector in question. If the Incident constitutes a crime punishable by the Swedish Criminal Code (or another Act where the penalty is imprisonment) the Swedish Police, the Swedish Prosecution Authority and/or the Swedish Security Service will investigate it, depending on the crime.

If the Incident concerns GDPR-related issues, i.e. personal data, the Swedish Authority for Privacy Protection is the investigative authority.

If the Incident is influencing IT systems that provide critical infrastructure, e.g. traffic, the Swedish Civil Contingencies Agency is the investigative authority.

If a service provider fails to report an Incident, The Swedish Post and Telecom Authority constitutes the investigative authority.

If the Incident is connected to payment services, the Swedish Financial Supervisory Authority is the investigative authority.

Finally, it should be noted that, in December 2020, the Swedish government decided to establish a new national cybersecurity centre. Activities to establish the new authority are currently proceeding in co-operation between four Swedish security agencies – the Swedish Civil Contingencies Agency, the National Defence Radio Establishment, the Swedish Armed Forces and the Swedish Security Service. Tasks afforded to the new centre include, *i.a.*, coordinating activities to prevent, discover and handle cyber-attacks and other security Incidents, as well as warning systems relating to cyber-attacks. The centre is planned to be fully established in 2023.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Swedish law does not require organisations to implement backdoors or provide encryption keys.

Jonas Forzelius is one of the founders of Time Danowsky Law Firm and has more than 20 years' experience of advising clients in IT, outsourcing, intellectual property, and regulatory matters relating to IT-procurements and other commercial and public projects. He has extensive experience of assisting clients in both the public and private sector in complex projects, contract drafting, negotiations and regulatory advice, including cybersecurity matters and litigation.

Experience

- Partner, TIME DANOWSKY Advokatbyrå (since 2020).
- Partner, Time Advokatbyrå (2007–2020).
- Associate & Managing Associate, Linklaters Advokatbyrå (2001–2007).
- Associate, Lagerlöf & Leman Advokatbyrå, London (1999–2001).
- Law Clerk, Stockholm County Court (1999).
- Trainee, Lagerlöf & Leman Advokatbyrå (1998–1999).

TIME DANOWSKY Advokatbyrå AB
Birger Jarlsgatan 15
S-114 11 Stockholm
Sweden

Tel: +46 70 753 09 69
Fax: +46 8 23 99 80
Email: jonas.forzelius@timedanowsky.se
URL: www.timedanowsky.se

Esa Kymäläinen has over 20 years' experience of working in the areas of IP and IT law, data protection, regulatory issues and dispute resolution. Esa also has extensive experience of crisis management and as an advisor in connection with internal investigations and threat situations.

Experience

- Partner, TIME DANOWSKY Advokatbyrå (since 2020).
- Partner, Danowsky & Partners Advokatbyrå (2012–2020).
- Associate, Danowsky & Partners Advokatbyrå (2000–2011).
- District Court Clerk, Stockholm City Court (2000).

TIME DANOWSKY Advokatbyrå AB
Birger Jarlsgatan 15
S-114 11 Stockholm
Sweden

Tel: +46 70 288 76 04
Fax: +46 8 23 99 80
Email: esa.kymalainen@timedanowsky.se
URL: www.timedanowsky.se

TIME DANOWSKY is a law firm with focus on today's business, where technology, innovation and media/content form a natural part of all our business activities.

We offer high-end legal expertise with focus on tech/IT, media and dispute resolution. Practice areas include all types of commercial legal matters, including contracts, M&A, outsourcing, protection of intellectual property rights, marketing, competition, public procurement and regulatory compliance.

Clients include distinguished companies and organisations in Sweden, as well as internationals doing business in the Nordic region or with companies within the Nordic region.

The firm's fundamental objective is to provide straightforward, result-oriented legal advice of the highest quality, with a focus on tech/IT, media and dispute resolution.

Practice areas

- Corporate commercial.
- Corporate sustainability and risk management.
- Dispute resolution.
- EU and competition.
- Information technology and technology.
- Data protection and integrity.
- Intellectual property, marketing and media.
- Mergers and acquisitions.
- Public procurement.
- Regulatory compliance.

www.timedanowsky.se

TIMEDANOWSKY

Switzerland


Dr. Oliver M. Brupbacher


Dr. Nicolas Mosimann


Dr. Claudia Götz Staehelin


Marlen Schultze

Kellerhals Carrard

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

According to art. 143bis Swiss Criminal Code (SCC), hacking may constitute a criminal offence: any person who obtains unauthorised access, by means of data transmission equipment, to a data-processing system that has been specially secured to prevent such access, may be prosecuted upon complaint and be liable for a custodial sentence not exceeding three years or a monetary penalty. Art. 143bis SCC was revised to reflect Switzerland's implementation of the Budapest Convention on Cybercrime.

Unauthorised access to another person's password-protected email account constitutes hacking and is punishable under art. 143bis SCC (BGer 6B_615/2014 and 6B_456/2007; *cf.* also BGE 130 III 28). According to a ruling by the Swiss Federal Supreme Court (FSC), it is irrelevant in the application of art. 143bis SCC how the offender came into possession of the password (BGE 145 IV 185).

Data theft is covered by art. 143 SCC: any person who for their own or for another's unlawful gain obtains data for themselves or another, which is stored or transmitted electronically or in some similar manner and which is not intended for them and has been specially secured to prevent their access, is liable for a custodial sentence not exceeding five years or a monetary penalty.

In 2020, there were 27 convictions for crimes under art. 143bis SCC and 10 convictions for crimes under art. 143 SCC in Switzerland.

Denial-of-service attacks

Denial-of-service attacks may constitute damage to data (art. 144bis SCC): any person who without authority alters, deletes or renders unusable data that is stored or transmitted electronically or in some other similar way, may be prosecuted upon complaint, and be liable for a custodial sentence not exceeding three years or a monetary penalty. There is no requirement that the process is irreversible; even the temporary denial of access is punishable. A custodial sentence of a minimum of one to five years may be imposed on an offender who has caused major damage. Other than hacking, this offence is prosecuted *ex officio*.

In 2020, there were 13 convictions for crimes under art. 144bis SCC.

Depending on the specific *modus operandi* of the attack, further criminal provisions may apply, including extortion (art. 156 SCC), misuse of a telecommunications installation (art. 179^{septies} SCC) or coercion (art. 181 SCC).

Phishing

Depending on the circumstances, phishing may be covered by multiple criminal offences under the SCC, in particular:

- Unauthorised obtainment of data (art. 143 para. 1, custodial sentence not exceeding five years or a monetary penalty).
- Unauthorised access to a data-processing system (art. 143bis para. 1, prosecution upon complaint, custodial sentence not exceeding three years or a monetary penalty).
- Obtainment of personal data without authorisation (art. 179^{novies}, prosecution upon complaint, custodial sentence not exceeding three years or a monetary penalty).
- Forgery of a document (art. 251, custodial sentence not exceeding five years or a monetary penalty).
- Computer fraud (art. 147, custodial sentence not exceeding five years or a monetary penalty; if offenders act for commercial gain, they are liable for a custodial sentence not exceeding 10 years or a monetary penalty of a minimum of 90 daily penalty units).
- Fraud (art. 146, custodial sentence not exceeding five years or a monetary penalty; if offenders act for commercial gain, they are liable for a custodial sentence not exceeding 10 years or a monetary penalty of a minimum of 90 daily penalty units; for the interplay with art. 147 *cf.* BGE 129 IV 22, at 4.2).

The fraudulent use of a trademark or a copyright-protected work may be prosecuted under art. 62 Trade Mark Protection Act or art. 67 Copyright Act, each of which provides for a custodial sentence not exceeding one year or a monetary penalty.

2019 saw the first prosecution and conviction for "voice phishing" (Federal Criminal Court (FCC) SK.2019.9). One hundred and twenty-nine cyber-/phishing investigations by the Office of the Attorney General of Switzerland were pending at the end of 2020.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Apart from the application of the specific criminal provisions applicable to denial-of-service and phishing attacks (*cf.* above), the infection of IT systems with malware may be prosecuted under art. 143bis SCC, which penalises hacking, and art. 144bis para. 1 SCC, which covers damage to data.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

According to the so-called "virus offence" (art. 144bis para. 2 SCC), any person who without authorisation manufactures,

imports, markets, advertises, offers or otherwise makes programs accessible, that they know or must assume will be used to cause damage to data (art. 144bis para. 1 SCC; *cf.* "Denial-of-service attacks" above), or provides instructions on the manufacture of such programs, is liable for a custodial sentence not exceeding three years or a monetary penalty. If the offender acts for commercial gain, a custodial sentence of a minimum of one to five years may be imposed. The FSC held that this provision also applies where the instructions have not been created by the offender, and even if they are incomplete, so long as they contain specific and relevant information for the manufacture of programs used to cause damage to data (BGE 129 IV 230).

Any person who markets or makes accessible passwords, programs or other data that they know or must assume are intended to be used to commit a hacking offence (art. 143bis para. 1 SCC; *cf.* "Hacking" above), is liable for a custodial sentence not exceeding three years or a monetary penalty (art. 143bis para. 2 SCC).

Possession or use of hardware, software or other tools used to commit cybercrime

The mere possession of such tools is not illegal.

Identity theft or identity fraud (e.g. in connection with access devices)

While not explicitly regulated, identity theft can be punishable under arts 143bis, 143 SCC (unauthorised access to a data-processing system and unauthorised obtainment of data; *cf.* "Hacking" above), arts 146, 147 SCC (fraud or computer fraud), arts 173–178 SCC (offences against personal honour), or art. 179^{novies} SCC (obtainment of personal data without authorisation).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Data theft is covered by art. 143 SCC (*cf.* "Hacking" above).

Further, the betrayal of a manufacturing or trade secret amounts to a criminal offence if the offender is under a statutory or contractual duty of confidentiality (art. 162 SCC). This offence may be prosecuted upon complaint and is punishable with a custodial sentence not exceeding three years or a monetary penalty.

Depending on the circumstances, political, industrial or military espionage (arts 272–274 SCC) may also apply. These offences are generally punishable with a custodial sentence not exceeding three years, a monetary penalty or, in serious cases, a custodial sentence of a minimum of one year.

A wilful breach of a professional duty of confidentiality (e.g. banking secrecy, medical secrecy or attorney-client privilege) concerning sensitive personal data collected in the exercise of the profession is punishable, upon complaint, with a monetary penalty (art. 35 Federal Act on Data Protection (FADP)).

Deliberate and unlawful copyright infringements are covered by arts 67 *et seqq.* Copyright Act and are punishable with a custodial sentence not exceeding one year or a monetary penalty.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Unsolicited penetration testing may qualify as hacking and be sanctioned under art. 143bis SCC (*cf.* "Hacking" above), given that this offence does not require an intent of unjust enrichment.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Beyond the above, notable other criminal offences, both general and sector-specific, include the following:

- Criminal mismanagement (art. 158 SCC): a custodial sentence not exceeding three years or a monetary penalty; or a custodial sentence of one to five years if the offender acts to secure an unlawful financial gain for himself or another.
- Participation in a criminal organisation (art. 260ter SCC): a custodial sentence not exceeding five years or a monetary penalty (*cf.* rulings on "cyber jihad/cyber terrorism" by the FCC (SK.2013.39) and the FSC (BGer 6B_645/2007)).
- Money laundering (art. 305bis SCC), which is of particular importance in connection with denial-of-service and ransomware attacks (*cf.* above): a custodial sentence not exceeding three years or a monetary penalty, in serious cases not exceeding five years or a monetary penalty whereby a custodial sentence is to be combined with a monetary penalty.
- Breach of official, postal or telecommunications secrecy and of professional confidentiality (arts 320 *et seqq.* SCC): generally, a custodial sentence not exceeding three years or a monetary penalty; further punishable breaches of confidentiality are covered in particular by art. 47 Banking Act, art. 147 Financial Market Infrastructure Act (FinMIA), and arts 43, 53 Telecommunications Act (TCA).
- Disruption of public services, in particular of the railway, postal, telegraphic or telephone services, or of a public utility or installation that provides water, light, power or heat (art. 239 SCC): a custodial sentence not exceeding three years or a monetary penalty.
- Falsification or suppression of information (art. 49 TCA): a custodial sentence not exceeding three years or a monetary penalty.
- Misuse of information (art. 50 TCA): a custodial sentence not exceeding one year or a monetary penalty.
- Unsolicited distribution of spam messages (art. 3 para. 1 lit. o, art. 23 Unfair Competition Act): a custodial sentence of up to three years or a monetary penalty.

Because IT security is regulated in Switzerland with respect to specific objects (data, systems and products) and industries, further criminal offences may apply, depending on the circumstances.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Generally, the above-mentioned offences have extraterritorial application only if they are also liable for prosecution at the place of commission (or the place of commission is not subject to criminal law jurisdiction), if the offender is located in Switzerland, and if he/she is not extradited (arts 6, 7 SCC).

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Sentencing under Swiss law is determined by multiple factors pertaining to the offender. Mitigating factors include: acting with honourable motives, under duress or in serious distress; excusable emotional strain; psychological stress; serious provocation; a show of genuine remorse, in particular if the offender has made reparations; or the time elapsed since the crime where the offender has exercised good behaviour (art. 48 SCC). Withdrawal from the act or active repentance are further potential mitigating factors (art. 23 SCC).

The competent authority shall refrain from prosecuting the offender, bringing him to court or punishing him if the level of culpability and the consequences of the offence are minor (art. 52 SCC).

Notably, "hacking" according to art. 143bis SCC does not require an intent of harm or unjust enrichment.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Cybersecurity Incidents may trigger the application of many different statutes. Rather than in a comprehensive manner, Switzerland regulates cybersecurity with respect to specific objects (data, systems and products) and specific industries. Moreover, minimum cybersecurity measures are rarely defined by law, but are left to self-regulation. There is hardly any case law to clarify the standards, either.

The 2018–2022 National Strategy for the Protection of Switzerland against Cyber Risks (NCS II) has acknowledged the need for greater standardisation and regulation across various objects and sectors. According to the Federal Council's September 2021 interim report, implementation is proceeding according to plan.

Among the general laws applicable in the cybersecurity field are the following:

- Civil Code.
- Code of Obligations (CO).
- SCC.
- Council of Europe Budapest Convention on Cybercrime of November 23, 2001 (ETS No. 185; in force in Switzerland since January 1, 2012).
- Employment Act.
- Unfair Competition Act.
- Copyright Act.
- Trade Mark Protection Act.

Among the object-specific or sector-specific laws are the following:

- FADP (revised Act approved by Parliament on September 25, 2020) and related Ordinance (the total revision of the Ordinance has been in the consultation process since June 23, 2021; both acts are expected to enter into force in the second half of 2022), as well as cantonal data protection laws.
- Revised Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108; not yet ratified and in force but approved by Parliament on June 19, 2020 – the referendum deadline expired on October 8, 2020 and ratification is subject to the entry into force of the new FADP).
- Product Safety Act.
- Product Liability Act.
- Banking Act and related Ordinance.
- FinMIA.
- Financial Market Supervision Act (FINMASA).
- Revised Therapeutic Products Act (entered into force on May 26, 2021) and related Ordinances.
- Electronic Health Records Act and related Ordinance.
- Revised Medical Devices Ordinance (MedDO) (main provisions entered into force on May 26, 2021).
- TCA and related Ordinance.
- Embargo Act.
- Revised Federal Act on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods (entered into force on January 1, 2021) and related Ordinance.
- Ordinance on the Export and Brokerage of Goods for Internet and Mobile Communication Surveillance.
- Intelligence Service Act.
- Ordinance on Protection against Cyber Risks in the Federal Administration.

In the globalised universe of cybersecurity, laws often have an extraterritorial effect. Foreign laws, such as the EU General Data Protection Regulation (*cf.* art. 3), may therefore have to be taken into account as well when assessing Incidents in Switzerland.

Provisions on cybersecurity may also include guidelines and standards. While generally non-binding, they may be taken into account when interpreting statutory provisions. They may also be declared binding by sector-specific associations or by reference in contracts. For example, the National Cyber Security Centre (NCSC) maintains an "Information security checklist for SMEs". The Federal Office for National Economic Supply (FONES) issued "Minimum standards for improving ICT resilience" for operators of critical infrastructures that may be adopted by interested private parties as well. Non-governmental initiatives include the Swiss Code of Best Practice for Corporate Governance and the International Organisation for Standardisation's ISO/IEC 27000 family of standards focusing on security of digital information, as well as its standard ISO/IEC 30141:2018 regarding IoT Reference Architecture.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Currently, there are no generally applicable mandatory cybersecurity requirements for critical or essential infrastructure and services. The regulation of cybersecurity for such infrastructure and services is fragmented and inconsistent, and it often lacks a precise definition of the required security measures (*cf.* question 4.2 below).

However, the need for further standardisation and regulation has been recognised in the NCS II, as adopted by the Federal Council on April 18, 2018. One of its focus areas remains the improvement of ICT resilience of critical infrastructures.

Accordingly, the 2018–2022 Critical Infrastructure Protection Strategy (CIP II) defines the overriding goals and principles of action for all parties involved, and identifies 17 measures to improve the country's resilience, *i.e.* its resistance, versatility and regeneration capacity, with regard to its critical infrastructures. The CIP II lists the following nine critical infrastructures for Switzerland: financial and insurance services; healthcare; telecommunications; and public administration (set out in greater detail in question 4.2 below), as well as: public transport; energy; food supply; waste management; and public security.

The draft of a new Federal Information Security Act was accepted by Parliament in December 2020 and is expected to enter into force by the end of 2021. It contains minimum requirements for the protection of information and IT infrastructure hosted by the federal authorities. The Ordinance on Protection against Cyber Risks in the Federal Administration entered into force on July 1, 2020. It regulates the organisation of the Federal Administration's protection against cyber risks as well as the tasks and responsibilities of the various offices in the cybersecurity domain, in particular the NCSC (*cf.* question 8.1 below).

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Other than for critical or essential infrastructures and services (*cf.* question 2.2 above) and sector-specific regulations (*cf.* question 4.2 below), there are currently no specific legal requirements with respect to the measures listed above.

Their implementation may instead be driven by general legal requirements that, depending on the circumstances, may include the implementation of some or all of the above measures. They include, notably, the overall responsibility for the due management of a company and individual professional confidentiality obligations as well as data protection requirements. Guidelines and standards may also include provisions on cybersecurity. While generally non-binding, they may be taken into account when interpreting statutory provisions. They may also be declared binding by sector-specific associations or by reference in contracts (*cf.* questions 5.1 and 5.2 below).

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Currently, Switzerland knows no general obligation to report Incidents or potential Incidents to the authorities. However, the introduction of such an obligation is contemplated as part of the federal government's NCS II. With the exception of in cases involving serious security incidents in critical infrastructures, Incident reporting is currently encouraged on a voluntary basis, typically via the recently established NCSC, which incorporates the former Reporting and Analysis Centre for Information Assurance (MELANI) and serves as a new national contact point (*cf.* question 8.1 below). Reports can be made through a message on the NCSC's website and can also be submitted anonymously. The NCSC's statistics for the second half of 2020 show a continued high activity in all areas of cybersecurity risk.

Illegal activity on the internet can also be reported to the Cybercrime Coordination Unit Switzerland (CYCO), which may forward the matter to the competent domestic and foreign law enforcement authorities.

Sector-specific regulations for critical infrastructures regularly require the reporting of serious security incidents without delay. The scope of serious security incidents generally extends beyond, but may include, Incidents. More precise criteria may be specified in non-binding guidelines that explain the regulator's intended enforcement practice and are regularly accepted and complied with by the industry. Among the most prominent cybersecurity reporting obligations for critical infrastructures are those for financial and insurance services (*cf.* art. 29 para. 2 FINMASA; Financial Market Supervisory Authority (FINMA) Guidance 05/2020; FINMA Circular 08/25), healthcare (*cf.* art. 12 para. 3 Electronic Health Records Ordinance; art. 66 revised MedDO), as well as telecommunications (art. 96 para. 2 Ordinance on Telecommunication Services) (*cf.* question 4.2 below).

In December 2020, the Federal Council instructed the Federal Department of Finance to prepare a consulting draft concerning the introduction of a reporting obligation for operators of critical infrastructure in the event of cyber-attacks and the discovery of security vulnerabilities. The Federal Council has set corresponding benchmarks for the design of the bill: a central reporting office is to be designated at the legislative level and defined uniformly for all sectors. The criteria for who is to report which incidents and within what timeframe are also to be defined. The concrete provisions on the structure of the reporting obligation are to be defined in corresponding decrees, adapted to the sector-specific circumstances. The reporting obligation should be coordinated with existing sectoral and data protection reporting obligations.

A specific reporting obligation for Incidents relating to personal data will be introduced by the revised FADP. Data controllers will have to notify the Federal Data Protection and Information Commissioner (FDPIC) as soon as possible of data breaches that are likely to result in a high risk for the personality or the fundamental rights of data subjects. Correspondingly, data processors will have to inform the data controller as soon as possible of any data breach. A notification of the FDPIC must at least refer to the nature of the data breach, its consequences, and any measures taken or planned. In any subsequent criminal proceeding, the notification may only be used against the notifying company or person with their consent (arts 24 paras 1–3 and 6 revised FADP; *cf.* art. 7 revised Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data).

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

There is currently no specific requirement under the FADP to notify data subjects of an Incident. Depending on the seriousness of the data breach, however, such a requirement may arise under the general principle of data processing in good faith (art. 4 para. 2).

The revised FADP will explicitly require data controllers to inform affected data subjects of a data breach if it is necessary for their protection or if the FDPIC – after having been informed of the data breach (*cf.* question 2.4 above) – so orders (art. 24 paras 1, 4 revised FADP). Exceptions will apply in particular in cases of overriding public or private third-party interests or where reporting would be impossible or require a disproportionate effort (art. 24 para. 5 lit. a, b revised FADP).

Further obligations to report Incidents or potential Incidents to affected individuals or third parties may derive from the generally required lawfulness of all data processing (art. 4 para. 1 FADP; art. 6 para. 1 revised FADP), as well as from specific contractual obligations.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

Where applicable, the general Incident reporting is overseen by the NCSC, CYCO, FDPIC, and the cantonal Data Protection Commissioners.

Sector-specific reporting is overseen by the respective regulatory authorities, most notably by the FINMA for financial and insurance services, by the Federal Office of Public Health (FOPH) for healthcare, and by the Federal Office of Communications (OFCOM) for telecommunications (*cf.* question 4.2 below).

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

For lack of a general reporting obligation for Incidents, there are currently no generally applicable penalties for non-compliance with reporting obligations.

Sector-specific sanctions may apply, such as in case of financial and insurance services, healthcare and telecommunications (*cf.* question 4.2 below). Under the revised FADP, object-specific sanctions will apply for violations of the minimum security requirements for personal data and for non-compliance with orders by the FDPIC (arts 8, 24, 61 lit. c, and 63).

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Cyber risks are a key part of the prudential supervision by the FINMA, which has stepped up its efforts in the area. These risks are monitored directly, for example through focused on-site audits by the FINMA, and monitored by audit firms as part of the regulatory audit process. In 2020, the FINMA strengthened its cyber risk resources and introduced a new cyber supervisory approach to monitor all supervised entities. The concept provides for supervision in the following areas: threat analysis; ongoing supervision; and incident response or crisis management.

In addition, larger institutions are regularly reminded of the need to take appropriate precautions against cyber risks during self-assessments. According to the FINMA's Annual Report 2019, self-assessments in the second half of 2018 focused on the ability of the participating institutions to identify cyber threats arising from institution-specific vulnerabilities, perform a commensurate risk assessment and define countermeasures (threat intelligence). The outcome of the self-assessments was that most of the participating institutions had made adequate provision for those risks. The FINMA's on-site supervisory reviews in 2020 focused, *inter alia*, on cyber risks and cybersecurity, including in the investment banking, asset management and insurance sectors.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

There is no law specifically allowing or prohibiting the use of beacons. However, companies that intend to use beacons for such purposes should analyse, in each case, whether their use is in compliance with Applicable Laws, including the SCC, the Unfair Competition Act and the FADP.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

There is no law specifically allowing or prohibiting the use of honeypots. Companies should, however, keep the same regulations in mind as with beacons.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)

There is no law specifically allowing or prohibiting the use of sinkholes. The same considerations apply as with beacons and honeypots.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Organisations may monitor the electronic communication of their employees, provided that they comply with the provisions pertaining to the processing of personal data in the CO (art. 328b) and the FADP. Consequently, such monitoring must, in particular, be: carried out lawfully; in good faith; proportionate (i.e. suitable, necessary and affecting the data subject's privacy in the mildest possible way); and known to the data subjects.

Depending on the circumstances, the monitoring of employee data can be justified on the basis of the employment contract, industry-specific laws applicable to the employer (e.g. in case of banks) or the overriding interest of the employer to prevent or detect cyber-attacks. Relying on employee consent as justification for the processing, however, entails certain risks due to the usually limited ability of employees to refuse consent. Under the principle of transparency, employers are recommended to issue a monitoring regulation setting out the specifics of the surveillance measures.

Ordinance 3 to the Employment Act prohibits surveillance and monitoring systems that monitor the behaviour of employees (art. 26). Employers must ensure that the health of employees is not affected by the monitoring. However, a non-personal – anonymous or pseudonymous – evaluation of employee data is usually sufficient in order to prevent cyber-attacks, and it is, in principle, lawful under this provision, even if conducted systematically. In certain individual cases (e.g. after a cyber-attack), an individualised analysis of employee data may also be permissible.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

The Federal Act on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods, as well as the respective Ordinance and Annexes, provide for certain import and export restrictions for dual-use goods, including technology and software. Annex 2, part 2, 4A005, 4D004 and 4E001.c set forth export restrictions for technology for the development of intrusion software, whereby certain exceptions exist with regard to vulnerability disclosures and reactions to cyber Incidents. Moreover, according to Annex 2, part 2, 5A002, systems for

information security and their components, including cryptographic technology for the confidentiality of data with a specific security algorithm, are subject to export restrictions.

Exceptions are available, such as for technology that is available to consumers, cryptographic technology for digital signatures, symmetric algorithms below 56 bit-encryption and many more. Furthermore, export restrictions may apply to equipment, and its components, for the interception and interruption of mobile communication and surveillance equipment (Annex 2, part II, 5A001.f), and to systems and equipment, and its components, for the surveillance of IP communication networks (Annex 2, part II, 5A001.j).

The Ordinance on the Export and Brokerage of Goods for Internet and Mobile Communication Surveillance must also be taken into consideration.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The Applicable Laws and market practice vary across the different business sectors in Switzerland. The NCS II has acknowledged the need for greater standardisation and regulation across the different sectors (*cf.* question 2.1 above).

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Financial and insurance services

The focus of cybersecurity regulations in Switzerland has traditionally been on its financial and insurance services sector.

Financial market infrastructures, as defined in art. 2 lit. a FinMIA (e.g. stock exchanges, multilateral trading facilities, payment systems), are obliged to operate IT systems that: ensure the fulfilment of the duties imposed by the FinMIA; are appropriate for the activities conducted; provide for effective emergency procedures; and ensure the continuity of the business activity (art. 14 FinMIA). Special IT systems requirements apply to financial market infrastructures with systemic importance in order to protect against the risks to the stability of the financial system (art. 23 FinMIA).

According to the FINMA, cyber risks are among the most significant operational risks for banks and insurance companies. Accordingly, they are required to implement appropriate risk management measures to tackle operational risks, including cyber risks, and must safeguard their infrastructure against various types of attacks (art. 3f para. 2 Banking Act; art. 12 Ordinance on Banks; and the non-legally binding FINMA Circulars 2008/21 "Operational Risks – Banks" and 2017/2 "Corporate governance – insurers").

Supervised persons and entities must immediately report Incidents that are of substantial importance to the supervision to the FINMA (art. 29 para. 2 FINMASA; FINMA Guidance 05/2020; FINMA Circular 08/25). Violations of the reporting obligations may face sanctions, including: a custodial sentence of up to three years or a monetary penalty for the wilful provision of false information or the omission of reporting to the FINMA; a fine of up to CHF 250,000 in case of negligence (arts 45 *et seq.* FINMASA); and a revocation of the licence, a withdrawal of the recognition or a cancellation of the registration in case of serious infringements (art. 37 FINMASA).

Healthcare

Cybersecurity in the healthcare sector has recently received increased attention in Switzerland, in particular in view of the cybersecurity risks relating to the electronic patient record and medical devices connected to the internet.

The first electronic patient records were certified at the end of 2020. Certification requires a risk-based data security and data protection system, the technical and organisational specifications of which are defined by the FOPH. Relevant security Incidents have to be notified to the FOPH. The violation of these requirements may lead to a suspension or removal of the certification (art. 12 para. 1 lit. b Electronic Health Records Act; art. 12, 38 para. 1 Electronic Health Records Ordinance).

In line with the developments in the EU, in particular the Medical Devices Regulation 2017/745 of April 5, 2017 (MDR), Switzerland has revised its MedDO, the main provisions of which entered into force on May 26, 2021. Accordingly, medical devices have to fulfil the general safety and performance requirements in Annex I of the MDR, both with respect to hardware and software (art. 6 paras 1, 2 MedDO). Manufacturers of medical devices may have to notify severe Incidents as well as their corrective measures (art. 66 MedDO).

Telecommunications

Another emphasis of cybersecurity regulations lies on the telecommunications sector.

The OFCOM issued the non-binding "Directives on the security and availability of telecommunication infrastructures and services" (based on art. 96 para. 2 Ordinance on Telecommunications Services (OTS)). They specify security requirements and define minimum security levels that each telecommunication services provider should maintain in order to contribute to the reliability and availability of the national telecommunications network. With the revision of the TCA (entered into force January 1, 2021), a specific obligation to protect against cyber-attacks was introduced (art. 48a revised TCA).

Telecommunications service providers are required to immediately inform the OFCOM of faults in the operation of their networks that affect a relevant number of customers (art. 96 para. 1 OTS). Such disturbances may also result from cyber-attacks. Failure to report may result in a fine not exceeding CHF 5,000 (art. 53 TCA).

Federal Administration

The draft of a new Federal Information Security Act was accepted by Parliament in December 2020 and is expected to come into force by the end of 2021. It contains minimum requirements for the protection of information and IT infrastructure hosted by the federal authorities.

The Ordinance on Protection against Cyber Risks in the Federal Administration entered into force on July 1, 2020. It regulates the organisation of the Federal Administration`s protection against cyber risks as well as the tasks and responsibilities of the various offices in the cybersecurity domain, in particular the NCSC (*cf.* question 8.1 below).

Other important sectors

Further sector-specific regulations apply, including for critical infrastructures. The NCS II and CIP II aim to implement measures to improve cybersecurity across various sectors on the basis of periodically updated risk and vulnerability analyses (*cf.* questions 2.1 and 2.2 above).

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

As a general principle, the primary responsibility for cybersecurity lies with the organisation (*cf.* question 5.2 below) rather than with the individuals entrusted with the task.

The board of directors, managing directors and executive officers of companies limited by shares, as well as the managing directors of limited liability companies, have a duty of loyalty and care and in particular a non-transferable and inalienable responsibility for the overall management of the company, the company's organisation, including accounting and financial controls, as well as the overall supervision of the persons entrusted with managing the company (arts 716a, 717, 810, 812 CO). Hence, the ultimate responsibility for the cybersecurity strategy of such companies, including the adoption of an appropriate organisation and of the necessary directives, processes and controls, lies with the respective management. In light of the increasing importance of cybersecurity, management must either have the requisite know-how itself or obtain relevant advice and cannot simply delegate the task to the IT department. Accordingly, if such companies suffer loss because of an Incident that results from an intentional or negligent breach of their duties, management may become personally liable both to the company and to the individual shareholders and creditors (arts 754, 827 CO).

The current FADP does not provide for sanctions for breaches of data security (art. 7). As of the expected entry into force of the revised FADP in 2022, however, the company's management or – if data security has been internally delegated – its data protection officer, IT manager or compliance officer may face fines of up to CHF 250,000 for intentional violations of the statutory minimum data security requirements (art. 8 para. 3, art. 61 lit. c. revised FADP).

Criminal sanctions against individuals may also apply under various other, including sector-specific, laws, notably for intentional breaches of professional confidentiality (e.g. art. 35 FADP/art. 62 revised FADP; arts 320 *et seqq.* SCC), but also at times for negligence (e.g. art. 47 Banking Act; arts 43, 53 TCA; art. 16 Product Safety Act).

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Other than for critical or essential infrastructures and services (*cf.* question 2.2 above) and in sector-specific regulations (*cf.* question 4.2 above), there are currently no specific legal requirements with respect to the IT security measures listed above. Their implementation may instead be driven by general legal requirements that, depending on the circumstances, may include the implementation of some or all of the above IT security measures. They include, notably, the overall responsibility for the due management of a company and individual professional confidentiality obligations (*cf.* question 5.1 above) as well as data protection requirements.

Privacy by design requires that the confidentiality, availability, and integrity of personal data must be protected through adequate technical and organisational measures, taking into account the purpose, nature, and extent of the data processing, the possible risks and the current state of the art. The measures must be reviewed periodically. More specific requirements apply for the automated processing of personal data (arts 7 FADP and 8 *et seq.* Ordinance to the FADP; arts 7, 8 revised FADP). The revised FADP will introduce additional obligations to maintain an inventory of processing activities and to conduct privacy impact assessments (arts 12, 22).

Beyond the applicable regulations, guidelines and standards may also include provisions on cybersecurity (*cf.* question 2.1 above). While generally non-binding, they may be declared binding by sector-specific associations or by reference in contracts. They may also be taken into account when interpreting statutory provisions. For example, manufacturers of data-processing systems or programs, as well as private persons or federal bodies that process personal data, may obtain a data protection certification (art. 11 FADP). The applicable standard in such cases is ISO/IEC 27001:2013.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There is currently no specific requirement under the FADP to notify the public of an Incident. Depending on the seriousness and on the number of affected data subjects, however, the general principles of lawful and good-faith data processing (art. 4 paras 1, 2 FADP; *cf.* also art. 6 paras 1, 2 revised FADP) may require an Incident to be reported publicly (*cf.* questions 2.4 and 2.5 above). This option is explicitly foreseen in the revised FADP (art. 24 para. 5 lit. c).

If Incidents or cybersecurity risks lead to the expectation of a future cash outflow, a company may be required to book the probably required provisions and charge them to the profit and loss account (*cf.* art. 960e CO or other applicable financial reporting standards).

Companies listed on the SIX Swiss Exchange are subject to specific periodic disclosure requirements (art. 49 *et seq.* Listing Rules (LR)). They may also have to consider whether an Incident amounts to a qualified reportable event and, hence, triggers *ad hoc* publicity obligations (art. 53 LR; Directive on Ad Hoc Publicity). Whether an Incident represents a qualified reportable event has to be assessed on a case-by-case basis, considering whether it has a substantial impact on the development of a company's share price and therefore has the potential to influence average investors in their investment decision.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Liability is a key consideration in cybersecurity. While legally possible, civil action against cybercriminals will regularly prove unfeasible. In practice, the focus is therefore on secondary liability: entities affected by an Incident may turn to the provider of a defective product or service; and third parties suffering damage from the Incident may look to the affected organisation for having failed to comply with appropriate data security standards.

In case of a contractual relationship that contains a respective IT security representation, the third party (client, supplier,

etc.) can bring a contractual liability claim against the organisation affected by the Incident, provided it can demonstrate a breach of contract, damage, causation as well as fault (arts 97 *et seqq.* CO). The latter is generally presumed, which is why it is for the defendant to prove that it was not at fault with respect to the Incident. Special contractual liability provisions may provide for strict liability, such as in case of direct losses caused to a buyer (art. 208 para. 2 CO).

If there is no IT security representation, the defendant's fault will be assessed against a standard of due care and the related threshold question of what level of cybersecurity is reasonable and appropriate to avert damage from a third party, taking into account the level of risk, applicable industry standards, and the state of technology.

General commercial terms often contain liability limitations for third-party actions and consequential damages. It is questionable whether such general terms would be upheld in the event of an Incident, and any advance exclusion of liability for gross negligence would in any case be void (art. 100 para. 1 CO). Difficult questions may also arise where a multitude of parties contribute, albeit unintentionally, to an Incident.

For liability based on tort, or other civil wrongs independent of contract (*cf.* question 6.3 below).

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

There is no published case law in relation to Incidents for a failure to comply with appropriate data security standards or the delivery of defective security products or services.

Since Swiss law currently remains unfriendly to mass claim proceedings, data subjects affected by a security breach will, in most cases, encounter difficulties in asserting financial damages in an amount that merits a claim.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

In the absence of a contractual relationship (*cf.* question 6.1 above), entities may incur liability in tort, or *another* civil wrong independent of contract, for the harm that an Incident causes to third parties, irrespective of contractual disclaimers or limitations of liability.

General tort law provides relief for damages caused by an illicit act, whether wilfully or negligently (such fault not being presumed; arts 41 *et seqq.* CO). An illicit act exists in case of a breach of an absolute right of the victim (personality, intellectual property or similar rights) or a financial damage resulting from the breach of a specific legal provision that is designed to protect against such damage, which must be determined on a case-by-case basis. Disgorgement of profits arising from a cyber-attack may be sought based on unjust enrichment or on agency without authorisation (arts 62 *et seqq.*, 423 CO).

In the software and IoT context (e.g. hacked medical devices, cars, etc.), product liability rules may be of particular relevance: if a defective product, which does not provide the safety that would reasonably be expected, leads to an Incident, the manufacturer, importer or supplier is, in principle, strictly liable for personal injuries and damage to privately used property caused by the product (arts 1, 4 Product Liability Act).

If a company limited by shares or a limited liability company suffers loss because of a severe data breach that results from a lack of appropriate internal cybersecurity controls and procedures, the respective board members, managing directors and executive officers may become personally liable to both the company and the individual shareholders and creditors for any loss or damage arising from an intentional or negligent breach of their duties (arts 754, 827 CO; *cf.* question 5.1 above).

To the extent an Incident due to insufficient data protection or data security leads to a violation of personality rights, such as in case of data theft or illegal data processing, affected persons may bring an action seeking, e.g. damages, moral compensation, disgorgement of profits, injunctions and notification to third parties or publication (art. 15 para. 1 FADP/art. 32 para. 2 revised FADP; arts 28 *et seqq.* Civil Code; arts 41 *et seqq.*, 49, 423 CO).

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Organisations in Switzerland are permitted to take out insurance against Incidents, and insurers have offered cyber products for a number of years already. The respective offerings often close a coverage gap as many property and liability insurance policies exclude cyber risks.

Cyber insurance solutions are very much customised and can include almost every cyber risk, including denial-of-service and ransomware attacks, costs of internal investigations and crisis management, recovery of stolen, destroyed or damaged data, reputational damage, and the defence against third-party claims. The implementation of a customary and up-to-date cyber risk management and respective protective measures are a necessary condition of admission and coverage under many cyber insurances. Unless contractually excluded, art. 14 para. 2 Insurance Contract Act entitles the insurer to reduce its coverage in case of gross negligence of the insured.

In addition to the high degree of customisation, many key coverage terms have not been analysed by the courts, and cyber risks are complicated and constantly evolving. Accordingly, foreign cases such as *Mondelez International, Inc. v. Zurich American Insurance Co.*, No. 2018L011008, 2018 WL 4941760 (Ill. Cir. Ct., Oct. 10, 2018) have also been monitored closely in the jurisdiction.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are not.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Switzerland does not have a central enforcement agency for cybercrimes. Instead, prosecution of the various cybercrimes lies with the competent police departments and public prosecutors' offices on cantonal and federal level. Equally, while reporting duties for serious security events, including Incidents, exist for critical infrastructures such as finance and insurance, healthcare and

telecommunications, there is currently no general and specific duty to notify cybersecurity breaches (*cf.* question 2.4 above).

The NCSC, headed by the Federal Cyber Security Delegate, is Switzerland's cybersecurity competence centre (*cf.* Ordinance on Protection against Cyber-Risks in the Federal Administration of July 1, 2020). Its aim is to enable the Confederation to play a more active role in protecting the country against cyber risks by supporting the general public, businesses and educational institutions as well as public administrations in their protection against cyber risks, by improving the security of the Federal Administration's own infrastructure. The MELANI, together with the national Computer Emergency Response Team (GovCERT), have been integrated into the NCSC as a national contact point and technical expertise hub. Incident reporting to the MELANI is voluntary. Upon receipt of a report, the MELANI will analyse it and provide assessments and recommendations. The MELANI can adopt an active lead role where an Incident jeopardises the proper functioning of the Federal Administration.

The CYCO at the Federal Office of Police (FEDPOL) is Switzerland's central office for anyone who wishes to report illegal activity on the internet. It also actively investigates illegal internet activity. The CYCO does not prosecute the matters itself but, after a first review and data backup, passes them on to the competent domestic and foreign law enforcement authorities.

Switzerland is a member of the Budapest Convention on Cybercrime. Besides committing its member states to increase their national efforts to effectively fight cybercrime, the Convention fosters increased, rapid, and well-functioning international cooperation.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No, there are not.

Dr. Oliver M. Brupbacher is a partner at Kellerhals Carrard. He represents clients in litigation and arbitration in commercial matters as well as in investigations. He specialises in healthcare and life sciences, cross-border proceedings and mutual legal assistance, as well as data protection and information governance. He also advises clients on cybersecurity prevention and crisis management. As a former Senior Litigation Counsel, Head of Global Discovery and a global product lawyer at Novartis, Oliver Brupbacher combines deep expertise in his areas of practice with an intimate understanding of the industry and of clients' needs at all organisational levels, in both domestic and international contexts.

Kellerhals Carrard
Henric Petri-Strasse 35, P.O. Box 257
CH-4010 Basel
Switzerland

Tel: +41 58 200 30 00
Fax: +41 58 200 30 11
Email: oliver.brupbacher@kellerhals-carrard.ch
URL: www.kellerhals-carrard.ch

Dr. Nicolas Mosimann is a partner at Kellerhals Carrard. His practice focuses on M&A, corporate law, technology and intellectual property law and commercial law. He advises both Swiss and international companies and institutions on transactions (e.g. acquisitions, joint ventures, financing rounds, licences and outsourcing) and technology projects (e.g. IoT and blockchain-based platforms), research and cooperation agreements, commercial contracts and data protection (including the EU GDPR). In addition, Nicolas specialises in advising both providers and customers on software and cloud projects. Moreover, as a founding member and co-head of the Startup Desk of Kellerhals Carrard, Nicolas knows the needs of founders and their companies in the seed and growth phases.

Kellerhals Carrard
Henric Petri-Strasse 35, P.O. Box 257
CH-4010 Basel
Switzerland

Tel: +41 58 200 30 00
Fax: +41 58 200 30 11
Email: nicolas.mosimann@kellerhals-carrard.ch
URL: www.kellerhals-carrard.ch

Dr. Claudia Götz Staehelin, head of the Kellerhals Carrard Investigation practice group, is a litigation and investigation partner and specialises in international dispute resolution, as well as internal investigations across various industries. She advises her clients in compliance, internal investigations, cross-border proceedings, international mutual legal assistance and data privacy (CIPP/E), and supports her clients in dispute resolution crisis management. Claudia is also active as an arbitrator. Claudia combines investigation and dispute resolution expertise with significant business experience. Before joining the firm, Claudia was the head of litigation at Novartis, where she led large multi-jurisdictional disputes and investigations and advised senior management on company litigation risks, as well as on financial and reputational impact.

Kellerhals Carrard
Henric Petri-Strasse 35, P.O. Box 257
CH-4010 Basel
Switzerland

Tel: +41 58 200 30 00
Fax: +41 58 200 30 11
Email: claudia.goetz@kellerhals-carrard.ch
URL: www.kellerhals-carrard.ch

Marlen Schultze is a member of the Kellerhals Carrard White-Collar Crime practice group at Kellerhals Carrard. She has extensive experience in criminal law and criminal procedural law, with a focus on white-collar crime and the prevention of corruption and money laundering. In addition, she advises clients on compliance and conducts internal investigations.

Kellerhals Carrard
Henric Petri-Strasse 35, P.O. Box 257
CH-4010 Basel
Switzerland

Tel: +41 58 200 30 00
Fax: +41 58 200 30 11
Email: marlen.schultze@kellerhals-carrard.ch
URL: www.kellerhals-carrard.ch

With more than 220 legal professionals (consisting of partners, of counsels, associates, tax advisors and notaries) and more than 400 employees, the firm, which has its origins in 1885, is one of the largest and most traditional law firms in Switzerland, with offices in Basel, Bern, Geneva, Lausanne, Lugano and Zurich, and representative offices in Binningen, Sion, Shanghai and Tokyo.

Kellerhals Carrard advises and represents companies and entrepreneurs from all industries and economic sectors, public authorities, national and international organisations and private individuals before all judicial and administrative bodies nationally and abroad in practically all areas of the law. Our activities are focused on:

- Company and corporate law, external legal department.
- Litigation, arbitration and insolvency law.
- M&A and capital markets law.
- Regulatory financial markets law, financial services, collective investments, leasing, insurance.
- IT/IP, distribution, competition and anti-trust law.
- International sports law.
- Tax.
- Public law.
- Employment and social insurance law.
- Commercial criminal law and international mutual assistance/compliance.
- Family and inheritance law for private customers.
- Notarial office.

Kellerhals Carrard focuses in particular on the areas of financial services, life sciences, IMT (Information, Technology and Media), sport, energy, real estate/construction, as well as on trading and retail.

www.kellerhals-carrard.ch

Kellerhals Carrard

Taiwan

Lee and Li, Attorneys-at-Law

Ken-Ying Tseng

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Pursuant to Article 358 of the ROC Criminal Code, a person who breaks into someone else's computer or related equipment by entering another's account code and password without authorisation, breaks into a protection measure, or takes advantage of a loophole of such system shall be sentenced to imprisonment for no more than three years or short-term imprisonment; *in lieu* thereof, or in addition thereto, a fine of no more than NTD300,000 may be imposed. Hacking, i.e., the unauthorised access of another's system, is likely to be deemed as constituting such an offence.

Denial-of-service attacks
Pursuant to Article 360 of the ROC Criminal Code, a person who, without authorisation, interferes with the computer or related equipment of another person and causes injury to the public or another through the use of computer programs or other electromagnetic methods shall be sentenced to imprisonment for no more than three years or short-term imprisonment; *in lieu* thereof, or in addition thereto, a fine of not more than NTD300,000 may be imposed. "Denial-of-service attacks" may be deemed as such unauthorised interference of another's computer system and may be subject to the above criminal sanctions.

Phishing
Pursuant to Article 359 of the ROC Criminal Code, a person who, without authorisation, obtains, deletes or alters the magnetic record of another's computer or related equipment and causes injury to the public or others shall be sentenced to imprisonment of no more than five years or short-term imprisonment; *in lieu* thereof, or in addition thereto, a fine of no more than NTD600,000 may be imposed. "Phishing" in general refers to the activities of obtaining someone else's important information, such as account number and password, or personal information, by using the internet, which may constitute the above offence if injury to the public or others is caused.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infection of IT systems with malware may be deemed as interfering with another's computer system and altering the records in another's computer system without authorisation and may be deemed as the offences set forth under Article 360 and/or Article 359 of the ROC Criminal Code and may be subject to the criminal sanctions as set forth above.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Pursuant to Article 362 of the ROC Criminal Code, a person who makes computer programs specifically for themselves or another to commit the offences specified as set forth under Articles 358 to 361 of the ROC Criminal Code and causes injury to the public or another shall be punished with imprisonment of no more than five years or short-term imprisonment; *in lieu* thereof, or in addition thereto, a fine of no more than NTD600,000 may be imposed. The mere distribution, sale or offering of software that may be used to commit cybercrime may not be deemed as constituting the offence as set forth under Article 362 of the Criminal Code. Whether a person will be held criminally liable with regard to possessing such software will depend on the actual activities that the person conducts by possessing or using such software.

Possession or use of hardware, software or other tools used to commit cybercrime
Please see above.

Identity theft or identity fraud (e.g. in connection with access devices)
Depending on how the identity information is stolen, the activity to obtain the identification information may constitute either the offence set forth under Article 358 or Article 359 of the ROC Criminal Code as set forth above. As for using another's identity for fraud purposes, it may constitute either the general criminal offence concerning "fraud" activity as set forth under Article 339 of the ROC Criminal Code or depending on the factual situation, constitute the criminal offence set forth under Article 339-3 of the ROC Criminal Code, which stipulates that a person who for the purpose of exercising unlawful control over other's property for themselves or for a third person takes the property of another by entering false data or wrongful directives into a computer or relating equipment to create the records of acquisition, loss or alteration of property ownership shall be sentenced to imprisonment for no more than seven years; in addition thereto, a fine of no more than NTD700,000 may be imposed. Tricking an automated machine, such as an ATM, by stealing someone else's identity is a separate criminal offence under the ROC Criminal Code. Pursuant to Article 339-2, such activity may incur criminal sanction, such as imprisonment for no more than three years and/or a criminal fine of no more than NTD300,000. Whether the activities concerning identity theft or identity fraud would constitute any other criminal offence shall depend on the actual activity that was conducted.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Under Taiwan law, either infringing another's copyright or trade secret may incur criminal liabilities. In addition, an individual breaching the confidentiality obligations that he/she was imposed with during his/her prior employment relationship with his/her former employer may incur civil liability for breach of contract. If the confidential information constitutes a trade secret of the former employer, the individual may be subject to a criminal sanction of up to five years' imprisonment or short-term detention, and a criminal fine ranging from NTD1 million to NTD10 million may be imposed. If the purpose of the infringement of a trade secret is for the trade secret to be implemented or exercised in the PRC, Hong Kong or Macau, the individual may be subject to imprisonment of one to 10 years and a criminal fine of NTD3 million to 50 million may be imposed. As for infringing another's copyright, depending on the actual infringement being conducted, the amount of the criminal fine may be as high as NTD5 million, and the length of imprisonment may be as long as five years.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Depending on the relevant facts, such activity may be deemed as constituting one or more criminal offences as listed above.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Depending on the actual fact concerning such activity, such activity may be deemed as constituting one or more criminal offences as listed above. For example, in 2016, a group of Russians and Eastern Europeans hacked into the system of a Taiwan bank from London and remotely accessed and controlled certain ATMs of the Taiwan bank located in Taiwan and obtained cash from the machines. The individuals came to Taiwan to collect the cash, which was then seized by the Taiwan police, while the hackers outside of Taiwan remain untouched. The Russian and Eastern Europeans who were seized by the Taiwan law enforcement authorities were sentenced to criminal sanctions including imprisonment for having committed almost all of the above-mentioned criminal offences.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The relevant statutes do not "spell out" any extraterritorial application but whether those will have extraterritorial application shall be subject to the general provisions under the ROC Criminal Code. If the relevant actions cause any consequence in Taiwan or one of the elements of the actions is conducted in Taiwan, the Taiwan court will have jurisdiction over such offences and the ROC Criminal Code will become applicable.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

The relevant statute does not stipulate any specific reporting or notification mechanism that can exempt the offender from the relevant penalties. It seems that other than "surrendering himself/herself" to the law enforcement authority, there is no other mechanism that can reduce the criminal liability.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The following Taiwan statutes may be relevant to cybersecurity:
1. Cybersecurity Management Act ("CMA");
2. Personal Data Protection Act ("PDPA");
3. Criminal Code (the relevant offences with regard to computer crime and fraud, etc.);
4. Communication Security and Surveillance Act;
5. Trade Secret Act;
6. Copyright Act;
7. Patent Act;
8. National Security Act;
9. Counter-Terrorism Financing Act; and
10. Regulation Governing Export and Import of Strategic High-Tech Commodities.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Yes, other than the CMA and the relevant regulations or rules promulgated pursuant to the CMA, there are a few statutes and regulations promulgated by the authority regulating the telecommunications industry with regard to the designation of critical infrastructure and the relevant security level, which basically follow the principles set forth under the CMA.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The CMA requires Taiwan government agencies as well as the specific non-government agencies to adopt cybersecurity maintenance plans and report any cybersecurity Incident to the relevant government authorities. Each of the competent authorities has issued guidelines for adopting cybersecurity plans in this regard for the reference of the businesses that are subject to their jurisdictions. In such guidelines, general security standards, including ISO27001, were referred to and recommended. Although, in such general securities standards, there is no reference to the specific obligation that shall be imposed on a government agency or a non-government agency with regard to the monitoring, detecting, preventing or mitigating the occurrence of any Incidents, reference to implementing anti-virus measures or adopting periodical checks on the security procedures were made. In sum, the obligations that a government agency or a specific non-government agency is imposed with are a general security obligation.

With regard to personal data protection, a private organisation is required to take proper security measures to protect the personal data that it holds so that the personal data will not be stolen, altered, damaged, or lost. The competent authority of

each industry has the power to require the private organisations under its jurisdiction to stipulate personal data file security maintenance plans.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Pursuant to the CMA, the agencies subject to the Act shall report to their supervisory agency or to the competent authority of the industry that the private agency is engaging in as applicable when the agency becomes aware of a cybersecurity Incident. A cybersecurity Incident refers to any Incident under which the system or information may have been accessed without authorisation and used, controlled, disclosed, damaged, altered, deleted, or otherwise infringed, affecting the function of the information communication system and thereby threatening the cybersecurity policy.

The "Regulations for Reporting and Responding to Cybersecurity Incidents" set forth further details about the reporting of a cybersecurity Incident as required under the CMA. A "specific non-government agency" shall report to its regulator at the central government within "one hour" after it becomes aware of the cybersecurity Incident and the regulator shall respond within two to eight hours depending on the classification of the cybersecurity Incident. Meanwhile, the specific non-government agency shall complete damages control or recovery of the system within 36 to 72 hours depending on the classification of the cybersecurity Incident.

When making such a report to the authority, descriptions such as the time when the Incident occurs and when the agency becomes aware of the Incident, what had actually happened, the assessment of the risk level, the responsive measures that have been taken; the evaluation of any assistance from outside resources; and other relevant matters shall be included.

There are no specific provisions with regard to exemption of the reporting requirements, and it is not necessary for the authority to make such report publicly available.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

There are no such legal requirements under the CMA. However, under the PDPA, if there is any data breach Incident, a data controller shall notify the affected data subjects after it has the opportunity to inspect the relevant Incident. In the notification to the data subjects, the data controller shall briefly describe the data breach Incident and the corrective measures that the data controller has taken to protect the data subjects.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The sectoral regulators at the central government level in Taiwan are in charge of enforcing the relevant matters with regard to cybersecurity matters. With regard to personal data protection, either the sectoral regulators at the central government level or the municipal governments have the power to enforce the PDPA.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

With regard to cybersecurity, a private organisation that has been designated as a provider of the critical infrastructure may be ordered to take corrective measures by a certain deadline or it may be imposed with an administrative fine ranging from NTD100,000 to NTD1 million for its failure to comply with the obligations to (i) stipulate the relevant cybersecurity management plan, (ii) stipulate the responsive measures that should be taken in a cybersecurity Incident, or (iii) report the Incident to the relevant authority or submit the relevant investigation report, etc. and may be imposed with such fine consecutively until correction measures are taken.

With regard to a personal data breach Incident, if a private organisation fails to take proper security measures to protect the personal data that it retains or breaches its obligation to notify the data subjects affected by the personal data breach Incident, the competent authority has the power to order the private organisation to take corrective measures, and if no corrective measure is taken before the designated deadline, the authority has the power to impose an administrative fine ranging from NTD20,000 to NTD200,000 consecutively until corrective measures are made.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

As the CMA was recently implemented, thus far, no enforcement examples have been found. As for the PDPA, given that the enforcement power lies in the competent authority in charge of each different industry and there are no comprehensive methods to search such precedents, it is difficult to evaluate the level of the actual enforcement of each authority. The Financial Supervisory Commission (the "FSC"), however, has made the relevant enforcement decisions, which are online for public access. Based on the search in the FSC's database, there have been quite a few financial institutions being imposed with administrative fines for their failure to adopt proper security measures to protect the personal data that they retain or failure to notify the affected data subjects with regard to particular security Incidents.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

There is no specific law or statute permitting or prohibiting an organisation from taking such a measure to protect its IT

system. We believe that as long as the implementation of such technology will not be deemed as one of the criminal offences as described under section 1 above, an organisation shall be permitted to take such a measure.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There is no specific law or statute permitting or prohibiting an organisation from taking such a measure to protect its IT system. We believe that as long as the implementation of such technology will not be deemed as one of the criminal offences as described under section 1 above, an organisation shall be permitted to take such a measure.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There is no specific law or statute permitting or prohibiting an organisation from taking such a measure to protect its IT system. We believe that as long as the implementation of such technology will not be deemed as one of the criminal offences as described under section 1 above, an organisation shall be permitted to take such a measure.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Yes. Employee monitoring practices are permitted if (i) the employees no longer have a reasonable expectation of privacy, and (ii) such monitoring is not expressly prohibited by law. Employees are deemed not to have a reasonable expectation of privacy if their employer has expressly announced the monitoring policy and/or employees have consented to the monitoring. Furthermore, employees are deemed to have given an implied consent if they continue to use the equipment provided by the employer after the employer has announced the monitoring policy.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Taiwan follows the same practice of the international society with regard to the restriction on importation and exportation of encryption technology. We basically follow the principles set forth by the relevant international organisations, such as the "Nuclear Suppliers Group", the "Australia Group", as well as the relevant international conventions, such as "the Wassenaar Arrangement" and the "Chemical Weapons Convention".

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, different sectors implement different standards. For example, the regulators of the financial industry stipulate quite a few information security requirements and standards with specific security requirements, while the regulators of other industries may stipulate only general standards.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

With regard to the financial industry, there are various information security regulations and rulings requiring the financial institutions to take sufficient cybersecurity measures so as to protect their customers. For example, there are specific security standards for securities firms to offer "online" trading services to their customers, for banks to offer "online" banking services to their customers, and for insurance companies to offer insurance policies online.

As for the telecommunications sector, the competent authority, i.e., the National Communications Commission ("NCC"), also stipulates the relevant information security standards and measures and requires telecommunications operators to adopt and follow the standards. The NCC also took certain measures to encourage telecommunications operators to maintain their information security, such as holding training sessions and seminars.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Directors bear "fiduciary duty" to the company and will be held liable when they breach such duty to the company. A company's failure to prevent, mitigate, manage or respond to an Incident may not necessarily lead to the conclusion that their directors have breached their fiduciary duty. Under Taiwan law, directors are in charge of making business decisions for a company by forming the joint decision of the board, but they are not responsible for implementing any business decisions or the daily operation of the company. With regard to cybersecurity Incidents, it would depend on the internal rules of a company as to whether such an Incident shall be reported to the board of directors. If the management has reported an Incident to the board of directors pursuant to the internal rules, but the board of directors fails to take proper action to address or resolve the Incident or even try to conceal or cover up the Incident, the board of directors may be held liable.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

It is not mandatory under Taiwan law for a company to designate a CISO. Other than the specific non-government agency as designated by the relevant competent authority or the regulated companies, such as financial institutions or telecommunications operators, a company is not legally required to stipulate a written Incident response plan or policy, conduct periodical cyber risk assessments, or perform penetration tests or vulnerability assessments.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

No, unless such risks or Incidents are major or material to the operation of a listed company.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

In an Incident under which the computer system of a private organisation was hacked or invaded by others and the private organisation therefore suffered loss or damage, the private organisation, being the victim of the Incident, may file a civil lawsuit against the hacker or the other relevant wrongdoers either based on a tort claim or an unjustified enrichment claim, especially if there have been criminal proceedings launched against the hacker or the relevant wrongdoers at the same time. The private organisation, being the plaintiff, needs to establish the facts with regard to how the system was attacked, invaded or altered and how such activities can be linked to the hacker or the wrongdoers. The private organisation will also be required to substantiate the amount of the actual damage and the causation between the occurrence of the actual damage and the hacking activities.

Such a private organisation should also be able to file a civil action against the vendor that provided the IT/cybersecurity services to the private organisation if the vendor has failed to perform the required services or has failed to meet the required security standard. In this regard, the private organisation is required to establish that the vendor bears such an obligation to provide it with a security service meeting a certain level or standard based on the relevant contract as well as substantiate the actual amount of the damage.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

Since 2016, there have been quite a few "business email compromise" ("BEC") Incidents and many civil lawsuits were filed with the Taiwan court. Many of the cases involve a cross-border BEC scheme, under which a foreign company sought civil relief at the Taiwan court against individuals in Taiwan. Such individuals offered their bank accounts as the nominee accounts to receive the improper funds for the real hackers and their identities were discovered through the records in the banking system. The Taiwan law enforcement authority then worked with the foreign law enforcement authority to seize the nominee accounts and track down the individuals offering the nominee accounts. The nominee account holder would be held criminally liable under Taiwan law, either for being the accomplice of the hacker or breaching the Money Laundering Control Act. The victim would then bring a civil lawsuit against the nominee account holder. There are also court cases under which the nominee account holders were not found or criminally indicted but still the court ruled in favour of the victims against the nominee account holders and declared that the nominee account holders shall return the improper gain to the victims.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Under the PDPA, where a company fails to take proper security measures and thus causes the illegal disclosure of the personal data files they keep, they may be held civilly liable by the affected data subjects; this civil liability is by nature a tort liability under Taiwan law. In respect of the application of the general tort theory against a company that failed to prevent an Incident, this shall be determined on a case-by-case basis.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, they are permitted to do so.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no such regulatory limitations.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

If the police suspect or become aware of a certain crime being conducted in relation to an Incident, the police have the power to conduct an investigation of the suspect by requiring the suspect or third party to provide the relevant "information" to the police. If the police intend to seize the hardware or devices, the police would need to prepare all collected evidence for the prosecutor and request the prosecutor to apply with the court for the issuance of a search warrant to seize the hardware or devices. The court will review the warrant application submitted by the prosecutor. If the evidence collected by the police meets the standard of probable cause, the court, in most cases, would issue the search warrant.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no such specific statutes under Taiwan law.

Ken-Ying Tseng established Lee and Li's personal data protection practice group in 2012. In 2021, she combined the firm's TMT and data privacy practices and established a new practice group: Digital, TMT, and Data Privacy. Ken-Ying received an LL.M. from Harvard Law School. Ken-Ying constantly advises various tech companies that are in the businesses of social networks, instant messengers, search engines, portal sites, sharing economy, e-commerce, OTT, online gaming, P2P lending, e-payments, cloud computing, and so on. Ken-Ying also frequently advises clients, including multinational companies, on privacy and data protection (GDPR), e-marketing, big data, e-signatures, domain names, telecommunications, satellite, fintech, cybersecurity, internet governance, and other legal issues.
In addition, being the head of the firm's M&A practice group for more than 10 years, Ken-Ying assisted and represented several multinational corporations in their M&A activities, including BASF, Henkel, Yahoo!, Arrow, Bureau Veritas, Aleees, Sony, Micrel, Energy Absolute, Live Nation (Ticketmaster), Qualcomm and McDonald's, among others.

Lee and Li, Attorneys-at-Law
8F, No. 555, Sec. 4, Zhongxiao E. Rd.
Taipei 11072
Taiwan

Tel: +886 2 2763 8000
Email: kenying@leeandli.com
URL: www.leeandli.com

Lee and Li, Attorneys-at-Law is a full-service law firm and the largest law firm in Taiwan. Its history can be traced back to the 1940s. Lee and Li has formed practice groups that span corporate and investment, banking and capital markets, trademark and copyright, patent and technology, and litigation and ADR. Its services are performed by over 100 lawyers admitted in Taiwan and more than 100 technology experts, patent agents, patent attorneys, and trademark attorneys. Lee and Li was recognised as the "Taiwan Firm of the Year" or the "National Law Firm of the Year" by *IFLR* in 2001–2020. Lee and Li has also been recognised by other international institutions as the best law firm in the region, including *Who's Who Legal, China Law & Practice, Leaders League, Chambers and Partners, Asialaw* Regional Awards, etc.

www.leeandli.com

Thailand


Dr. Jason Corbett


Koraphot Jirachocksubsin

Silk Legal

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Gaining unauthorised access to a computer system is considered a criminal act, and offenders accused of doing so face up to six months' imprisonment and/or a fine of up to THB 10,000 (Computer Crime Act of 2017 ("**CCA**"), s.5). Likewise, perpetrators accused of accessing computer data without authorisation also face up to two years' imprisonment and/or a maximum fine of THB 40,000 (CCA, s.7).

Unauthorised access or security breaches against computer data or systems used to maintain national, public, and economic security, as well as infrastructure serving the interest of the public, are punishable by imprisonment for a maximum term of seven years, as well as a maximum fine of THB 140,000. Furthermore, if the crime results in damages to the computer data or system, the offender will be liable to a maximum prison term of 10 years and a fine up to THB 200,000 (CCA, s.12).

Denial-of-service attacks
An offender who blocks, defers, obstructs, or interferes with a computer system belonging to another person that causes it to fail to perform its normal function will be liable to a maximum prison sentence of five years and/or a maximum fine of THB 100,000 (CCA, s.10). If the offence results in damages to the other persons or their property, the offender will also face a maximum prison term of 10 years and a maximum fine of THB 200,000 (CCA, s.12/1).

Phishing
Whoever deceitfully inputs data into a computer system that is wholly or partly distorted, forged, or false in a manner that may likely cause damages to the public (except in cases that involve defamation) faces a maximum prison sentence of five years and/or a maximum fine of THB 100,000. If the offence is committed against a private person, the offender will be liable to imprisonment not exceeding three years and/or a fine of up to THB 60,000. It should be noted that phishing is considered a compoundable offence (CCA, s.14/1).

In addition, a service provider that cooperates, consents, or tacitly supports phishing activities by allowing the use of a computer system under their control will also be subject to the same penalties mentioned above.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Those found to have wrongfully damaged, destroyed, revised, modified, or made additions to data that belong to another person shall be liable to imprisonment for a term not exceeding five years and/or a fine of up to THB 100,000 (CCA, s.9).

Blocking, deferring, obstructing, or interfering with a computer system that belongs to another person that causes it to fail to perform regular functions is punishable by imprisonment for up to five years and/or a maximum fine of THB 100,000 (CCA, s.10).

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Disposing or distributing hardware, software, or other tools that were used to commit offences under the CCA is punishable by a maximum prison sentence of two years and/or a fine of up to THB 40,000 (CCA, s.13). Additionally, the offender responsible for disposing or distributing such tools will face greater penalties if they are found to have been aware of the intention to use the distributed tools for committing criminal acts under the CCA.

Possession or use of hardware, software, or other tools used to commit cybercrime
Failing to obey a court order calling for the destruction of data or software may result in criminal penalties deemed appropriate by authorities under s.14 and s.16 of the CCA (CCA, s.16/2), depending on the damages caused.

Moreover, officials may issue an order to surrender data or equipment used to store them. Those who fail to comply with such order will be liable to a fine not exceeding THB 200,000 on top of a daily fine capped at THB 5,000 until they comply with the order (CCA, s.18(5) and s.27).

Identity theft or identity fraud (e.g. in connection with access devices)
Committing identity theft is classified as cheating and fraud in Thailand, and offenders are subject to imprisonment not exceeding five years and/or a fine of up to THB 100,000 (Criminal Code, s.342(1).

Additionally, those illegally using an electronic or digital identification card belonging to another person will face imprisonment up to five years and/or a fine not exceeding THB 100,000 (Criminal Code, s.269/5). Notably, such an act is viewed as a cause of damage to the data of another person (CCA, s.9).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
This is considered a crime that carries the same penalties specified under the Criminal Code. Current or former employees who steal digital property or breach confidence are liable to a prison term not exceeding six months and/or a fine of up to THB 10,000 (Criminal Code, s.323).

Additionally, anyone found to have taken advantage of their position to steal another person's secret, discovery, or invention to benefit themselves faces a prison term of up to six months and/or a fine not exceeding THB 20,000 (Criminal Code, s.324). The offender may also be subject to criminal infringement under the Copyright Act (2015) and Trade Secret Act (2002).

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Currently, there are no specific laws surrounding penetration testing and whether it constitutes as ethical hacking.

Penetration testing is a simulated cyber-attack on a designated computer system for the purpose of evaluating its security and is performed on a contractual basis with permission from the computer system's owner. According to CCA, s.7, unsolicited access to a computer system or data, or doing so beyond the permission granted by the owner, is considered an offence.

Any other activity that adversely affects or threatens the security, confidentiality, integrity, or availability of any IT system, infrastructure, communications network, device or data
Those privy to security measures who disclose information that may likely cause damage to another person may face imprisonment for up to one year and/or a fine not exceeding THB 20,000 (CCA, s.6). Moreover, those who use digital tools to intercept the transmission of another person's private data may be subject to a prison term not exceeding three years and/or a fine of up to THB 60,000 (CCA, s.8).

Sending data or emails to any other person using a fake or concealed identity that hinders the use of their computer is punishable by a fine of up to THB 100,000 (CCA, s.11). Additionally, a person who sends out unsolicited emails or data in a manner that causes annoyance to the recipient, particularly when the sender does not provide ways or acknowledge requests to stop receiving emails, may be liable to a fine not exceeding THB 200,000. If such acts are done against public interest or security, the offender may also be subject to s.12 of the CCA.

Those who input false data that may cause harm to public security, cause widespread anxiety, or are otherwise considered integral to activities defined by the Criminal Code as terrorism or threats to national security may face imprisonment of up to five years and/or a maximum fine of THB 100,000 (CCA, s.14(2), (3)). Furthermore, service providers found to have directly or indirectly collaborated with offenders shall be liable to the same penalties above (CCA, s.15).

Regarding personal data, Thailand's yet to be enforced Personal Data Protection Act (2019) ("**PDPA**") prohibits the collection, use, or disclosure of personal data without consent.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes. However, they are subject to certain conditions under the Criminal Code whereby the nationality of an offender, and whether extradition treaties exist between Thailand and other corresponding jurisdictions, are taken into consideration.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Service providers found to have directly or indirectly provided consent or support in carrying offences under s.14 (see the question 1.1) will be exempt from incurring penalties under s.15 of the CCA, provided they can prove that they have complied with the Ministerial Notification; in particular, by notifying the relevant authorities of such incidents and stopping the use of their computer systems to commit offences.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Primary regulations that apply to cybersecurity in Thailand include:
1. the Criminal Code;
2. the CCA;
3. the Cybersecurity Act of 2019 ("**CSA**").
4. the PDPA (expected to be enforced in June 2022);
5. the Electronic Transactions Act of 2001;
6. the Financial Institutions Businesses Act of 2008 ("**FIBA**");
7. the Telecommunications Business Act of 2001 ("**TBA**"); and
8. the Payment Systems Act of 2017 ("**PSA**").

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The Critical Information Infrastructure defined under the CSA includes operations important to national, military, and economic security, as well as public order. The Organisation of Critical Information Infrastructure ("**CIIO**") shall provide assistance to prevent, cope with, and mitigate risks from cyber threats, particularly those targeting or affecting Critical Information Infrastructure.

CIIOs are businesses that have been tasked with providing services in the following aspects:
1. national security;
2. substantive public service;
3. banking and finance;
4. information technology and telecommunications;
5. transportation and logistics;
6. energy and public utilities;
7. public health; and
8. others as prescribed by the National Cybersecurity Committee ("**NCC**").

The NCC is authorised to appoint the coordinating agency for the CIIO to coordinate, monitor, cope with, and resolve cyber threats prescribed by law related to the Critical Information Infrastructure Supervising or Regulating Organisation ("**SRO**") (CSA, s.50). In this regard, the SRO is responsible for reviewing

the minimum cybersecurity standard of the CIIO and notifying the CIIO if it does not comply with the prescribed cybersecurity standards.

If there is a significant cyber threat to a system that belongs to a CIIO, the CIIO must report to the Office of the NCC ("**NCC Office**") and the SRO, and continue monitoring the threat.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

CSA

The CIIO must conduct a risk assessment on maintaining cybersecurity and periodically submit a summary report to the NCC Office. They must also establish a mechanism or process to monitor cyber threats or cybersecurity incidents relevant to its Critical Information Infrastructure (CSA, s.54, s.56).

PDPA

According to the upcoming PDPA, a data controller/processor is required to take security measures to monitor, detect, prevent, or mitigate any unauthorised or unlawful losses, access to, use, alteration, correction, or disclosure of personal data. In the event of a data breach, the data controller of a CIIO must notify the Office of the Personal Data Protection Committee ("**PDPA Office**") within 72 hours of becoming aware of the incident.

In certain industries, specific requirements may also apply to organisations; for example, telecommunication licensees must obtain protection and security measures pertaining to personal data, both technical and internal management protocols, with aspects suitable with the type of telecommunications services under the TBA.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

CSA

The CIIO must report any significant cyber threats on its system to the NCC Office and the SRO (CSA, s.57). However, no criteria or methods for reporting have been issued by Cybersecurity Regulating Committee ("**CRC**") at the time of writing.

PDPA

Those handling data have an obligation to notify the PDPA Office of data breaches within 72 hours of becoming aware of the incident, unless the breach poses little risk to the rights and freedoms of those whose data have been unlawfully breached. As such, the person who possesses the data must also notify those affected by the data breach. They must also implement remedial measures prescribed in their data policy without delay. However, specific rules and procedures have yet to be issued by the PDPA Committee, and the Act is not yet in force.

Other laws

According to the PSA and the Securities and Exchange Act of 1992 ("**SEA**"), information regarding incidents or potential incidents must be reported by operators, particularly payment service providers and securities companies, to relevant regulators.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Please see question 2.4 regarding the PDPA above.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

Regulators vary by sector; however, the following are considered relevant to the aforementioned requirements:

1. the PDPA Committee (upon its appointment) under the upcoming PDPA;
2. the Bank of Thailand ("**BOT**") regulating financial institutions and e-payment service providers;
3. the Securities and Exchange Commission of Thailand ("**SEC**") regulating securities companies;
4. the CRC regulating the CIIO; and
5. the National Broadcasting and Telecommunications Commission ("**NBTC**") regulating telecommunication service companies.

Law enforcement officers and state attorneys also play important roles in investigations or proceedings surrounding cybercrime offences.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

A CIIO that fails to report cyber threats (as mentioned in question 2.4) without reasonable cause may be subject to a fine not exceeding THB 200,000.

PDPA

Upon the enactment of the Act, a fine of up to THB 3,000,000 may be imposed on those who hold or collect data and do not comply with the notice requirements highlighted in questions 2.3, 2.4, and 2.5.

SEA

Securities companies that do not comply with the notice requirements mentioned in questions 2.4 and 2.5 face a fine of up to THB 300,000, together with a daily fine capped at THB 10,000 levied throughout the non-compliance period. Directors, managers, or any other responsible persons may also be liable to imprisonment for a term not exceeding six months and/or a fine of up to THB 200,000, unless it can be proven they were not involved with the offence.

FIBA

Failure to report to the BOT, as mentioned in our response to question 2.4, incurs a fine of up to THB 1,000,000 on top of a daily fine not exceeding THB 10,000 during the non-compliance period.

For e-payment service providers regulated by the BOT, the penalty for not complying with the notice requirement as indicated in our response to question 2.4 is a fine not exceeding THB 1 million or THB 2 million, depending on the type of e-payment service provider in question.

TBA
If a licensee fails to comply with the prescribed requirements or licensing conditions, the NBTC will order them to enact appropriate changes or perform remedial actions within a specified period. Failure to comply with an order issued by the TBA can lead to a minimum administrative daily fine of THB 20,000. The NBTC may also suspend or revoke licences if necessary.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

According to media reports, cyber attackers stole data belonging to 123,000 customers of Kasikorn Bank and Krungthai Bank in August 2018, the first large-scale data leak to have affected local financial institutions. It was reported the leaked information did not consist of financial data, and that both banks had already undergone measures to stop the breach, performed inspections on all related systems, and allowed experts to assess operating systems to ensure they were sufficiently protected. The BOT instructed the banks to tighten their cybersecurity systems, protect customers from the fallout, and inform the affected people. The BOT also ordered both banks to prepare measures for providing assistance in case damages were to arise at a later point.

Enforcement measures for failure to comply with the PDPA have also yet to be announced or clarified. Furthermore, no other significant non-compliance cases have been publicly taken in by relevant regulators, which is anticipated until at least until 1 June 2022 when the PDPA is expected to take effect.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There are no regulations preventing the use of Beacons to protect IT Systems in Thailand.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There are no regulations preventing the use of Honeypots to protect IT Systems in Thailand.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There are no regulations preventing the use of Sinkholes to protect IT Systems in Thailand.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Under the PDPA, an email address can be considered personal data given that it can be used to indicate a person's identity within a network. For purposes of facilitating an organisation's operations, they may be entitled to access employee emails and internet usage (if necessary) by obtaining consent from them. The rationale behind this could be that such organisations benefit from preventing and monitoring any suspicious activities that may clash with their security measures.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

There are currently no specific restrictions related to the import or export of technology. However, certain items may be subject to import-export restrictions of dual-use items.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

S.50 of the TBA provides the legal framework for the implementation of data protection and security measures. This framework covers technical and internal aspects regarding data security that is appropriate for each type of telecommunications services. Personal data protection and security measures must be implemented on a technical level based on the following requirements: (i) updating the encryption system for personal data at least every three months; and (ii) updating the level of security measures to comply with rapid changes in technological innovation.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Telecommunication service provider
The TBA requires telecommunication service providers to comply with technology information management and policies for personal data protection, as well as uphold rights to privacy and freedom in communication under the TBA. The NBTC sometimes imposes specific provisions concerning cybersecurity to each telecommunication service provider.

Financial service provider
Financial service providers must comply with the Notifications of the BOT regarding digital security measures and risk management.

Under the Payment Systems Act, e-payment service providers also need to follow the BOT's legal framework surrounding Business Continuity Management and Risk Assessments, specifically with regard to having a contingency plan or backup policy system to ensure service continuity, as well as safety policies and measures for the information systems used.

Other service providers

Other service providers may, at the discretion of regulators, comply with the governing legal framework to protect personal data. An example of this can be illustrated with insurance companies following the standard of the Office of Insurance Commission ("**OIC**"), or financial institutions complying with the Credit Information Business Operation Act of 2002.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Generally, if a data breach occurs under the supervision of an assigned Data Protection Officer, they must report the incident to the responsible persons within the organisation. If the director or any other responsible person fails to prevent, mitigate, manage, or respond to an incident, resulting in the organisation violating any regulations, the person will be held liable for the punishment of such offences. This legal aspect was the grounds for the CSA (s.77) and PDPA (s.81).

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

The CSA does not prescribe requirements for a Chief Information Security Officer ("**CISO**"). However, under the Notifications of the BOT, financial institutions that face high cybersecurity risks must appoint a CISO. Moreover, the CSA requires a CIIO to provide a cybersecurity policy, which covers risk assessments and response protocols for data breaches.

The CIIO must also provide a policy for implementing risk assessment for cybersecurity, including an examination from a cybersecurity standpoint by an information security auditor, internal auditor, or external independent auditor at least once a year (CSA, s.54). Moreover, the CSA (s.56) states that a CIIO must take part in organisational readiness assessments for dealing with potential incidents.

Once enacted, those handling consumer data under the PDPA must provide adequate security measures for personal data protection as required by the PDPA Office.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

The SEC requires securities firms to file annual reports to the SEC detailing their IT management and the occurrence of any incidents. Financial institutions and e-payment service providers must also create a report about their services and make them available for inspection by the BOT. The BOT can order financial institutions and e-payment service providers to give any information related to its services, including incident information.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Even though cybercrimes under various Acts face criminal liabilities, affected people can claim civil "damages" under the premise of a wrongful act (tort) for both wilful and negligent acts under s.420 of the Civil and Commercial Code ("**CCC**")

In addition, civil actions for compensation, including punitive damages, against those who hold customer data for breaches under the PDPA can be brought before the court once it has been enacted (PDPA, s.74).

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

As mentioned in question 6.1, there are a limited number of civil suits involving cybersecurity in Thailand that have been made available to the public for review.

As the PDPA has not taken effect in Thailand, there are no civil cases brought before the court under the PDPA.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes; please see our comments under question 6.1.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, the OIC allows insurance companies to sell "cyber insurance" policies to customers. The coverage of the policies mainly includes the theft of funds (i.e., money stolen on the internet executed by identity theft, phishing), cyber extortion, cyberbullying, online shopping scams, business interruption losses caused by security breaches, malware, ransomware, data recovery costs due to cyber-attacks, costs related to incident report and investigation, and subject to respective conditions thereto.

However, there are some conditions that the policy will not cover, depending on each insurance company. For instance, "the Company will indemnify the Insured for any loss or damage that the Insured cannot claim from the responsible person from other sources".

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are currently no regulatory limitations on insurance coverage against incidents as mentioned previously.

However, there are still no specific regulations or restrictions on either allowing or banning insurance policies covering any losses or damages resulting from digital asset transactions in Thailand. As of now, some digital exchange platforms in Thailand secure their companies and their digital assets by using international insurance companies.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

In order to prevent cybersecurity threats, the NCC may prescribe characteristics of various threats and classify them into: (i) cybersecurity threats that are not serious; (ii) critical cybersecurity threats; and (iii) crisis-level cybersecurity threats (CSA, s.60). In the event of a critical cyber threat, the CRC has the authority to require any relevant person to take charge of the following:

1. monitor computer systems;
2. examine computer systems to identify errors, analyse incidents, and evaluate the effects of potential threats;
3. conduct measures rectifying cybersecurity threats;
4. maintain the status of data and/or computer systems to conduct digital forensic analyses; or
5. access relevant computer data or other information related to the computer systems.

For a critical cybersecurity threat, the CRC also has the authority to assign an official to conduct the following, but only to the extent where it is necessary to prevent a cybersecurity threat:

1. enter a premises to examine relevant items;
2. access, copy, and filter data, computer systems, or programs;
3. test the operation of the computer system; or
4. seize or freeze a computer system or any other relevant equipment.

Certain orders require a court order, while others will not. However, orders must generally be limited to an extent where it is necessary to prevent or handle serious cybersecurity threats.

Other regulators (e.g., the BOT) are also authorised to investigate incidents.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Yes. According to the CCA, a service provider is obliged to retain computer traffic data for at least 90 days, but not exceeding two years from the date on which the data is imported into a computer system. In the event service is terminated, the service provider shall keep the users' data for a minimum of 90 days for service records usage. For the purposes of investigation, with respect to any offence under the CCA, officials are entitled to request from a service provider or relevant persons access such information.

Dr. Jason Corbett is the founder and Managing Partner of Silk Legal, who has advised clients on a variety of matters, including cross-border insolvency and restructuring, mergers and acquisitions, commercial transactions, fintech, and blockchain.
His interest and proficiency in matters pertaining to technology and innovation have made him a leader in providing cutting-edge solutions to solve the challenges found in the practice. Jason's notable competencies in this area have allowed him to assist investors, managers, and other stakeholders tackle a variety of legal, business, and intellectual property issues.
Moreover, with over 15 years of experience as an insolvency specialist, he has also assisted shareholders, creditors, receivers, trustees, and many others successfully conclude insolvency proceedings. His work has made him adept at formulating and executing out-of-court settlements that have bested inter-jurisdictional complexities. As the Thailand member of the International Insolvency Institute, he is considered one of the most sought-after legal counsel for creditors seeking to protect their interests in Thailand.

Silk Legal
RSU Tower, 8th Floor Suite 805
571 Sukhumvit Road (Soi 31)
North Klongton, Watthana, Bangkok, 10110
Thailand

Tel: +66 02 107 2007 ext. 310
Email: jason@silklegal.com
URL: www.silklegal.com

Koraphot Jirachocksubsin has handled matters that span across multiple practice areas, including corporate and commercial, Fintech, and real estate law, since 2014. During his tenure as an experienced Attorney, he has represented several prolific companies.
His previous experience includes leading due diligence and evaluation projects, as well as drafting and reviewing purchasing, structuring, licensing, and financing agreements. He is highly skilled in legal research and advising clients on new laws and regulations, including privacy and data protection, Fintech, and cybersecurity. He also has significant experience in dealing with small and medium enterprises (SMEs), in addition to larger corporations.
Since the beginning of his professional career, he has generously donated *pro bono* and time to charity. Lastly, his background includes financial and feasibility analysis work, allowing him to better serve clients who require this skill set.

Silk Legal
RSU Tower, 8th Floor Suite 805
571 Sukhumvit Road (Soi 31)
North Klongton, Watthana, Bangkok, 10110
Thailand

Tel: +66 02 107 2007 ext. 305
Email: koraphot@silklegal.com
URL: www.silklegal.com

Silk Legal is a boutique law firm that focuses on complex legal matters in Thailand. We are a full-service commercial law firm with dedicated practice areas in corporate and commercial, restructuring and insolvency, and regulatory matters. Our multi-national team provides clients with an international perspective of Thai law issues. Our approach is to fully explore your issues and offer you a global perspective, tailored to the local environment.
Our firm handles matters related to data privacy, specifically Thailand's PDPA, and cybersecurity. We are a proud member of PrivacyRules, an organisation that endeavours a hybrid approach when dealing with privacy, merging legal and technology to offer the broadest range of services. Silk Legal's Fintech practice combines a robust knowledge of industry best practices and emerging developments in the market. We also specialise in addressing complex regulatory and compliance matters surrounding blockchain and cryptocurrency.

www.silklegal.com

USA


Edward R. McNicholas


Kevin J. Angle

Ropes & Gray LLP

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Yes. The federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, is the primary statutory mechanism for prosecuting cybercrime, including hacking, and also covers some related extortionate crimes such as in the context of ransomware. The CFAA provides for both criminal and civil penalties (which in the criminal context can range from 10 to 20 years imprisonment for some aggravated offences, with the penalties for non-aggravated offences otherwise listed below), and specifically prohibits: (1) unauthorised access (or exceeding authorised access) to a computer and obtaining national security information (imprisonment up to 10 years); (2) unauthorised access (or exceeding authorised access) to a computer that is used in interstate or foreign commerce and obtaining information (imprisonment up to one year); (3) unauthorised access to a non-public computer used by the United States government (imprisonment up to one year); (4) knowingly accessing a protected computer without authorisation with the intent to defraud (imprisonment up to five years); (5) damaging a computer either intentionally or recklessly (imprisonment up to five years); (6) trafficking in passwords (imprisonment up to one year); (7) transmitting threats of extortion, specifically threats to damage a protected computer and threats to obtain information or compromise the confidentiality of information (imprisonment up to one year); and (8) cyber-extortion related to demands of money or property (imprisonment up to five years). In *Van Buren v. U.S.*, 140 S. Ct. 2667 (2020), the Supreme Court substantially limited the ability of the CFAA to penalise insider threats.

Other relevant laws applicable to cybercrimes include the Electronic Communications Protection Act ("ECPA"), which provides protections for communications in storage and in transit. Under the Stored Communications Act (Title II of the ECPA), 18 U.S.C. § 2702, it is a criminal violation to intentionally access without authorisation (or exceed authorised access) a facility that provides an electronic communications service ("ECS"), which could include, among others, email service providers or even some employer provided email. Violations of the ECPA are subject to penalties ranging from up to 10 years for repeat violations for an improper purpose. The ECPA also prohibits intentionally intercepting electronic communications in transit under the Wiretap Act (Title I of the ECPA), 18 U.S.C. § 2511, with some exceptions available for law enforcement, service providers and others (including, potentially, employers). The Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–1839, and the Defend Trade Secrets Act of 2016, 18 U.S.C. §§ 1836–1139, are further sources of potential criminal and civil penalties against the theft of trade secrets and other valuable intellectual property.

In addition to federal statutes, numerous states have passed statutes prohibiting hacking and other cybercrimes, some of which are broader than the federal statutes described. New York, for example, prohibits the knowing use of a computer with the intent to gain access to computer material (computer trespass), N.Y. Penal Law § 156.10, with penalties of up to four years' imprisonment. New York is merely one example; dozens of such state laws exist. Determining which statute is applicable depends on several factors under conflict of law rules, including the location of the alleged act and the location of the impacted individuals.

Denial-of-service attacks
Yes, a DOS attack could violate the CFAA, 18 U.S.C. § 1030(a)(5)(A) (intentionally damaging through knowing transmission, imprisonment up to 10 years), as well as state computer crime laws.

Phishing
Yes, among other statutes, phishing could violate the CFAA, 18 U.S.C. § 1030(a)(5)(A) or constitute wire fraud under 18 U.S.C. § 2702, which carries a potential sentence of up to 20 years' imprisonment.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Yes, planting malware would violate the CFAA, 18 U.S.C. § 1030(a)(5)(A) (intentionally damaging through knowing transmission, imprisonment up to 10 years), as well as state computer crime laws.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Conspiracy to commit an offence is often separately subject to criminal sanction. Whether distribution of hacking tools would constitute a crime would depend on whether the actor intended for them to be used for illegal purposes. If there were evidence of criminal intent, a person may be liable for aiding and abetting the violation of the CFAA, 18 U.S.C. § 1030(a)(5)(A), or related computer crime laws. With respect to federal statutes, aiding and abetting is subject to the same sentence as commission of the offence.

Possession or use of hardware, software or other tools used to commit cybercrime
As with distribution, mere possession of hacking tools would be difficult to prosecute in the absence of intent to use them for

illegal purposes or related conspiracy. If there were evidence of criminal intent or conspiracy and some overt act taken towards that end, a person may be liable for an attempt to violate the CFAA, 18 U.S.C. § 1030(a)(5)(A), or related computer crimes laws. With respect to federal statutes, attempt is subject to the same sentence as commission of the offence.

Identity theft or identity fraud (e.g. in connection with access devices)
Yes, identity theft could be charged under the federal identity theft statute, 18 U.S.C. § 1028, as well as numerous state laws.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Yes, electronic theft could violate the CFAA, 18 U.S.C. § 1030(a)(2) (obtaining information, without authorisation or exceeding authorisation, imprisonment of up to one year, or five if aggravating factors apply). It may also, or alternatively, violate the Economic Espionage Act, 18 U.S.C. §§ 1831–1839, which creates two crimes based on the theft of trade secrets; the first makes it a crime to acquire, without authorisation, trade secrets in order to benefit a foreign government, and the second if the theft will create economic benefit for others and will injure the target of the theft. While some courts previously held that obtaining information otherwise available on a computer system in violation of written policies prohibiting such access could constitute a violation of the CFAA, the Supreme Court recently found in *Van Buren v. U.S.* that violations of such purpose-based restrictions (i.e. restrictions imposed by contract or company policies) do not themselves constitute violations of the CFAA without other acts that exceed technical restrictions. 141 S. Ct. 1648 (2021).

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Yes. Unsolicited penetration testing could constitute a violation of the CFAA if the tester obtains data as a result or causes damage. To the extent information was obtained from the systems tested, such testing could violate 18 U.S.C. § 1030(a)(1) (national security information, imprisonment up to 10 years), (2) (obtaining information, imprisonment up to one year, or five if aggravating factors apply), or (3) (government computers, imprisonment up to one year). If the penetration tester causes damage, e.g. by impairing the integrity or availability of a system or data, the action could constitute a violation of § 18 U.S.C. § 1030(a)(5).

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
The CFAA, 18 U.S.C. § 1030(a)(2), and wire fraud statute, 18 U.S.C. § 2702, as well as numerous state laws apply to a wide variety of criminal conduct online.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes, the USA PATRIOT Act amended the CFAA and Access Device Fraud statute, 18 U.S.C. § 1029, to expressly apply them extraterritorially.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

The nature of the crime, whether it was intentional or unintentional, whether it was committed for economic benefit or malice or ethical hacking, and the number of past offences may impact the severity of any penalty. The existence of a robust corporate compliance programme, as well as cooperation with law enforcement, may help to mitigate any penalty or influence prosecutorial discretion.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Numerous federal and state laws include cybersecurity requirements. The Federal Trade Commission ("FTC") has been particularly active in this space and has interpreted its enforcement authority under § 5(a) of the FTC Act, applying to unfair and deceptive practices, as a means to require companies to implement security measures. The FTC has brought numerous enforcement actions against companies it alleges failed to implement reasonable security measures. The US Supreme Court, however, has recently circumscribed the FTC's abilities to seek monetary penalties for potential violations of the FTC Act without first utilising its administrative procedures.

Some federal laws, however, are sector-specific or extend only to public companies. Securities law generally prohibits fraud in connection with securities, and the Securities and Exchange Commission ("SEC") has been rigorous in the enforcement of disclosure requirements for adequate public disclosures regarding cybersecurity risks and material cybersecurity incidents. Moreover, the Gramm-Leach-Bliley Act ("GLBA") and its implementing regulations require "financial institutions" to implement written policies and procedures that are "reasonably designed" to ensure the security and confidentiality of customer records, and protect against anticipated threats and unauthorised access and use. The Health Insurance Portability and Accountability Act ("HIPAA") includes cybersecurity requirements applicable to protected health information in the possession of certain "covered entities" and their "business associates".

At the state level, many states have passed laws imposing security requirements. Most of these statutes require some form of "reasonable security". New York's SHIELD Act, for example, requires reasonable security for personal information and specifies measures that may satisfy that standard. The California Consumer Privacy Act ("CCPA") (expanded by the California Consumer Privacy Rights Act beginning in 2023) creates a data breach right of action for Californian residents with statutory penalties of $100 to $750 per consumer and per Incident if plaintiffs prove that the impacted business failed to implement reasonable security procedures to protect the personal information. Recently passed data protection laws in Virginia and Colorado also require "appropriate" security measures, and Massachusetts regulations have long imposed specific security requirements regarding personal information, including the implementation

of a written security programme and encryption of certain data. Regarding defensive measures, including a Company's ability to monitor for potential attacks, the Cybersecurity Information Sharing Act ("CISA") has two primary impacts. Firstly, it allows companies to monitor network traffic, including taking defensive measure on their own systems. Secondly, it encourages the sharing of cyber-threat information between companies and with the government.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The Cybersecurity and Infrastructure Security Agency Act created CISA, a component of the Department of Homeland Security, and the federal agency responsible for protecting critical infrastructure in the United States. CISA coordinates between government and private sector organisations in protecting critical infrastructure and has begun to develop and transmit information to private sector entities regarding its expertise in cybersecurity vulnerabilities, incident response and cybersecurity risk. As a recent example, along with the FBI and NSA, the agency published substantial information regarding the Conti ransomware, including technical details, attack techniques, and mitigations to reduce the risk of compromise. The federal government has also issued sector-specific guidance for critical infrastructure operators, and the nuclear, chemical, electrical, government contracting, transportation and other sectors have detailed statutory and regulatory requirements.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Generally, yes. U.S. cybersecurity laws exist at both the federal and state levels and vary by commercial sectors. For instance, several federal statutes have data breach notice provisions, but each state and four territories also have data breach laws. Many regulators expect regulated companies to have implemented "reasonable" security measures, taking into account factors such as the sensitivity of the data protected. In light of the proliferation of standards, many companies rely on omnibus cybersecurity frameworks like the NIST Cybersecurity Framework, covering efforts to identify and assess material foreseeable risks (including vendor security), design and implement controls to protect the organisation, monitor for and detect anomalies and realised risks, and respond to and then recover from Incidents.

In addition to general reasonable security requirements, some U.S. state laws or regulations are more prescriptive. For example, the New York Department of Financial Services Cybersecurity Regulation includes specific requirements such as annual penetration testing for covered entities.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes, all states and four territories have requirements for the reporting of Incidents and most of these statutes require reporting to state regulators. The nature and scope of the information that is required to be reported varies by state or territory. For example, California requires the following information in notices sent to individuals: (1) the name and contact of the reporting person; (2) a list of the types of personal information breached; (3) the date of the breach (or estimated range); (4) whether notification was delayed by a law enforcement investigation; (5) a general description of the breach incident (if possible); and (6) toll-free numbers and addresses of the major credit card reporting agencies.

These state requirements are in addition to federal requirements that are sector-specific. For example, the Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR") requires covered entities and business associates to report certain Incidents involving Protected Health Information ("PHI"). Public companies must also report material events.

Timeframes for reporting vary by state or agency, with most requiring notification around the same time that individuals are notified (or sometimes in advance). Vermont requires any notification to its Attorney General to be sent within 15 days. Covered financial institutions are required to report breaches to the New York Department of Financial Services within 72 hours. At the request of law enforcement agencies, however, some notifications may be delayed.

Information about cyber threats generally need not be reported, although the federal government encourages participation in Information Sharing and Analysis Centers ("ISACs") or Information Sharing and Analysis Organizations ("ISAOs") where threat intelligence is shared within sector-specific groups of companies.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

All 50 U.S. states and four territories have now passed breach notification statutes with varying requirements. Typically, breach notification statutes require notification be sent to individuals whose electronic Personal Information, as defined therein, was acquired in an Incident, though some states require notification based on access to such information alone. State definitions of Personal Information triggering data breach notification generally apply to the first name or first initial and last name in combination with another identifier, when not encrypted or redacted, such as social security number, driver's licence or identification card number, or account number, or credit card or debit card number in combination with any required security code, access code or password that would permit access to the individual's account. Increasingly, states are also including in the definition of Personal Information, health and biometric information, as well as usernames and passwords that provide access to

an online account. Many states also require that notice be sent to Attorney Generals or other state agencies, often depending on the number of individuals impacted. Most states allow for consideration of whether there is a risk of harm to the data subjects, but some states do not allow for such consideration.

Timeframes for notification vary by state; however, 30 days is a common standard. Additionally, some sector-specific laws provide notification requirements. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400–414, requires HIPAA-covered entities and business associates to provide notifications in the event of certain Incidents impacting PHI.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The regulator varies by sector, law and state. The FTC is the principal U.S. federal privacy regulator covering most for-profit businesses not overseen by other regulators. The SEC regulates many financial institutions and the OCR is primarily responsible for enforcing HIPAA. State Attorneys General have broad authority regarding enforcement of cybersecurity matters. In addition, federal and state regulators in particular sectors, such as insurance, have further enforcement powers.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

The U.S. has no single framework for non-compliance with notice requirements and penalties will depend heavily on the relevant law and regulator. In addition to regulatory penalties, private plaintiffs may file actions alleging non-compliance with relevant laws. For example, the CCPA provides for statutory damages of between $100 to $750 per consumer and per Incident in the event of a data breach caused by the failure to have in place reasonable security measures.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Hundreds of actions have been brought for non-compliance. For instance, Equifax agreed to pay at least $575 million as part of a settlement with the FTC, Consumer Financial Protection Bureau ("CFPB") and 50 U.S. State Attorneys General, or other state regulators charged with overseeing data security, related to its 2017 data breach allegedly impacting approximately 147 million people. Government authorities alleged that Equifax failed to have in place reasonable security for the information it collected and stored.

Typical of the FTC's enforcement is a case involving Uber in which it entered into an expanded settlement with Uber arising from a 2016 data breach, which the FTC alleged was not disclosed to the FTC for more than a year. The FTC had previously settled allegations related to an earlier 2014 breach. The FTC had alleged that Uber failed to live up to statements that access to rider and driver accounts were closely monitored, which, the FTC alleged, was not the case, rendering the statements false or misleading.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Generally, yes.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Generally, yes, subject to the CFAA.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Generally, yes, subject to the CFAA.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Yes, the CISA provides broad authorities to monitor network traffic, and employers can generally monitor employee communications where they first provide transparent notice of the monitoring and obtain consent from their employees.

Although the CISA may pre-empt them, state torts such as invasion of privacy may also limit an employer's ability to monitor employee communications, but tort law claims can be overcome where an employer can show that the employee did not have a reasonable expectation of privacy in the communication. Notices and consents to monitoring should be carefully drafted to ensure compliance.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Yes. Export Administration Regulations restrict the export of certain strong dual-use encryption technologies; however, licence exceptions may be available for exports.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Cybersecurity laws in the United States vary significantly by business sector. There is currently no single U.S. cybersecurity law of general application other than, arguably, restrictions

of "unfair" trade practices. Most businesses must comply with sector-specific federal and states laws. Healthcare organisations, for example, may need to comply with HIPAA, and many financial institutions are required to comply with the GLBA. Related state laws impose additional requirements.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Each of the sectors of critical infrastructure in the U.S. has its own separate regulatory regime. Energy, chemical, transportation and other sectors have detailed rules specific to their area. For example, in the financial services sector, financial services organisations must comply with the GLBA and its implementing regulations (which vary depending on the organisation's functional regulator). The SEC, other regulators and industry groups, such as the Financial Industry Regulatory Authority ("FINRA") and the National Futures Association ("NFA"), have published cybersecurity guidance that should be carefully reviewed. Red Flag Rules published by regulators require covered firms to adopt written programmes to detect, prevent and mitigate identity theft. The Fair Credit Reporting Act ("FCRA") and Fair and Accurate Credit Transactions Act ("FACTA") impose requirements with respect to credit reports. The FTC's Disposal Rule, 16 C.F.R. § 682, issued pursuant to FACTA, requires certain practices for the destruction of certain information contained in or derived from a credit report. State regulators sometimes impose very significant further regulations, particularly in New York. A different example would be the Communications Act, as enforced by Federal Communications Commission ("FCC") regulations, which requires telecommunications carriers and providers of Voice over Internet Protocol ("VoIP") services to protect "customer proprietary network information". Substantial fines and penalties can be assessed for failure to ensure adequate protections.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Public company boards of directors and officers owe shareholders fiduciary duties, including the duties of care and loyalty. To fulfil these duties, among other things, boards and officers must ensure that they are properly informed regarding the company's cybersecurity risks and the efforts the company has made to address them. Boards must also ensure that investors receive materially accurate disclosures of investment risk.

In the event of an Incident, boards and officers may face scrutiny and potentially litigation relating to their oversight of the company's cybersecurity. For example, in the Yahoo! data breach, individual board members and officers faced a shareholder derivative action alleging that they failed to exercise their fiduciary duties, failed to ensure that proper security measures were in place, failed to adequately investigate the Incident and made misleading statements. The allegations were ultimately settled for a reported $29 million. In that same Incident, the SEC issued a $35 million fine.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Federal and state laws may impose specific cybersecurity requirements that depend on the entity's functional regulator and the residence of the data subject. For example, the New York Department of Financial Services has issued regulations requiring covered financial institutions (which include banks and insurance companies) to, among other things, designate a CISO (or equivalent), establish a written Incident response plan and conduct a periodic risk assessment, annual penetration testing and biannual vulnerability assessments. Massachusetts information security regulations, likewise, require organisations that collect certain Personal Information from Massachusetts residents to implement a comprehensive information security programme that, among other things, identifies and assesses reasonably foreseeable internal and external risks to the security, confidentiality and integrity of such information. The New York SHIELD Act deems companies as compliant with its reasonable security requirement if they implement specified administrative, technical, and physical safeguards, including appointing an employee responsible for coordinating its cybersecurity programme and regularly testing the effectiveness of key controls, systems, and procedures. While not expressly required by regulation, the SEC has identified measures such as risk assessments, Incident response plans and penetration testing as elements of a robust cybersecurity programme for public companies and SEC registrants.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Public companies are required to publicly report material cybersecurity risks, including material past Incidents. Even if a past Incident is not material, companies should consider them in evaluating their disclosures regarding cybersecurity. The SEC has recently increased its enforcement activity regarding public company disclosures. For example, the SEC alleged that Pearson plc, a London-based education company, made misleading disclosures regarding cybersecurity risks as hypothetical when it had recently been made aware of a breach. The SEC has issued guidance regarding the factors public companies should report with respect to cybersecurity. Private companies do not have the same public disclosure obligations but may need to inform potential investors or purchasers regarding past Incidents or cybersecurity risks.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Organisations that publicly announce Incidents involving a large amount of Personal Information will often confront class action litigations filed by plaintiffs whose information was impacted by the Incident. Typically, these actions involve

several theories, including breaches of express or implied contracts, negligence, other common law tort theories, violations of federal or state unfair or deceptive acts or practices statutes or violations of other state and federal statutes, such as the CCPA.

Contract theories may involve claims of breach of contract where there is a written agreement between the plaintiff and the defendant that contains an express promise of reasonable security measures to protect personal information. Even if such a term is not included in the contract, many plaintiffs will assert a claim of implied contract, arguing that the receipt of a plaintiff's personal information implies a promise to protect the information sufficiently. Tort theories may involve negligence or other common law theories such as invasion of privacy, bailment, trespass to chattel, misrepresentations or unjust enrichment. Each of these theories may prove challenging to fit to the data breach context.

Consumer protection theories are often also alleged, claiming that a victim of a data breach committed unfair or deceptive acts or practices. Deception claims are typically premised on an alleged misrepresentation about the security practices of an organisation. Plaintiffs may also allege that a failure to protect information is "unfair"; although many courts will require a showing of substantial injury or widespread and serious consumer harm. Plaintiffs may also allege violations of other statutes such as the federal FCRA or other state laws.

In addition to establishing the elements of their claims, plaintiffs filing in federal court are required to show that they suffered injury-in-fact sufficient to establish standing. Even where an injury alleged is sufficient for standing, it may not be sufficient to state a claim for damages. Some damages theories that plaintiffs attempt to assert, with varying success, include risk of future identity theft, credit-monitoring costs, other costs related to mitigating risks related to an Incident and overpayment for the products and services associated with the Incident.

While most class actions involve plaintiffs whose information was allegedly compromised, there has been an increase in shareholder derivative and securities fraud actions arising from Incidents as well. In shareholder derivative actions, plaintiffs will typically allege that a company's officers and board of directors breached their fiduciary duties, wasted corporate assets or committed other mismanagement in failing to ensure that the company maintained what the plaintiffs consider appropriate security. As a preliminary step to any derivative action, plaintiffs must first either ask the board of directors to bring the action and, should the board refuse, prove that its refusal was contrary to the board's reasonable business judgment. Alternatively, they must prove that such a request would be futile. Both theories are difficult to prove.

Plaintiffs may also allege securities fraud. To do so, plaintiffs must allege that the company made materially false or misleading statements, typically regarding the state of its cybersecurity posture, and that the company knew about the falsity of such statements.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

As noted, the public announcement of an Incident will frequently result in class actions and other lawsuits being filed against the impacted organisation. Hundreds of actions have been filed over the years; some recent prominent examples include the following:

- Altaba (formerly known as Yahoo!): After announcing an Incident allegedly impacting up to 200 million people, faced consumer class action, shareholder derivative action and securities fraud action, in addition to regulatory investigations, which it ultimately agreed to settle.
- Home Depot: Suffered an Incident related to its payment card terminals. Home Depot settled actions brought by consumers and banks, which alleged that Home Depot had failed to implement adequate security measures. Home Depot also faced a derivative action, which was dismissed. On appeal, the action was settled after Home Depot agreed to adopt certain security procedures.
- Target: Suffered an Incident related to payment card data at its retail stores. Target faced consumer and shareholder actions and also an action brought by banks related to the theft of payment card data.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes, plaintiffs in data breach actions will often accuse the defendant of negligence or other tort law violations. A preliminary question any plaintiff must answer is whether there is any duty to protect the plaintiffs' information. The answer to that question may vary by state. Courts in several states have found no common law duty to protect personal information, while courts in other states have found such a duty under particular facts and circumstances. In *Dittman v. UPMC d/b/a The University of Pittsburgh Medical Center*, for example, the Pennsylvania Supreme Court found that an employer owes a duty to employees to use reasonable care to safeguard what the court described as the employee's "sensitive" personal data when storing it on an internet-accessible computer system.

The CCPA creates a data breach right of action for Californian residents with statutory penalties of $100 to $750 per consumer and per Incident if plaintiffs prove that the impacted business failed to implement and maintain reasonable and appropriate security practices.

In some states, defendants may assert the economic loss doctrine, which generally provides that contracting parties seeking damages for purely economic losses must seek damages in contract rather than in tort.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. Standalone cyber insurance policies typically cover both third-party liabilities arising from the defence and settlement of Incident-related claims, along with first-party cover for the policy holder's own losses, which could include investigation costs, legal fees, notification costs and the costs incurred in providing credit monitoring and identity theft services. Cyber insurance policy forms are typically not standardised and vary significantly from carrier to carrier. In light of the recent increase in ransomware and other cybersecurity incidents, cyber insurers are increasing rates and demanding more information about companies' security controls.

General liability or other policies may, in some instances, cover cyber-related losses, but costs related to Incidents are often excluded.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations specific to cyber insurance, but some states do not allow for insurance against certain violations of law.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Law enforcement retains numerous powers to investigate Incidents. In addition to standard warrant and subpoena powers, law enforcement may seek records stored by electronic communication services or remote computing services through the Stored Communications Act, intercept communications in transit through the Wiretap Act or obtain dialling or routing information through the Pen Register statute. The CLOUD Act authorises law enforcement to access certain information held by a United States-based service provider, even if the data is located in another country.

For Incidents involving national security or terrorism, law enforcement may have additional powers. Under the Foreign Intelligence Surveillance Act ("FISA"), the government can obtain information, facilities or technical assistance from a broad range of entities. National Security Letters ("NSLs") offer an additional investigative tool for limited types of entities.

Federal regulatory authorities such as the FTC, SEC and OCR have powers to investigate Incidents within their respective jurisdictions. State regulators may also investigate Incidents to determine whether any state laws were violated.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Under the Communications Assistance for Law Enforcement Act ("CALEA"), law enforcement requires certain telecommunications carriers and manufacturers to build into their systems or services necessary surveillance capabilities to comply with legal requests for information.

No general U.S. laws expressly require organisations to implement backdoors in their IT systems or provide law enforcement authorities with encryption keys. Under the All Writs Act, some courts in some instances have ordered reasonable assistance, including in one notable case, requiring Apple to provide assistance in circumventing security features – which Apple successfully resisted until it was moot.

Edward R. McNicholas is a co-leader of Ropes & Gray's privacy & cybersecurity practice. He represents technologically sophisticated clients facing complex data, privacy and cybersecurity issues. His clients include financial institutions, insurance companies, branded pharma companies, technology communications companies and select retailers. He is lead editor of the PLI Treatise, *Cybersecurity*. Recognised by the *National Law Journal* as a "Cybersecurity & Data Privacy Trailblazer", Ed has defended companies in dozens of significant data breaches. Mr. McNicholas previously served as an Associate Counsel to President Clinton, where he advised senior White House staff regarding various investigations. Mr. McNicholas received his J.D. from Harvard Law School, where he was an editor of the *Harvard Law Review*. He received his A.B. from Princeton University and served as a clerk at the U.S. Court of Appeals for the Fourth Circuit.

Ropes & Gray LLP
2099 Pennsylvania Ave, NW
Washington, D.C. 20006-6807
USA

Tel: +1 202 508 4779
Email: Edward.McNicholas@RopesGray.com
URL: www.ropesgray.com

Kevin J. Angle is counsel in the Ropes & Gray's privacy & cybersecurity practice. He represents a broad range of companies on privacy and cybersecurity compliance matters, incident response and transactional diligence. Kevin helps clients to anticipate and address potential areas of legal exposure and to structure privacy programmes to minimise potential liability. Kevin graduated from Columbia Law School and was an editor of the *Columbia Law Review*. After law school, he completed a clerkship for then Chief Judge Carol Bagely Amon of the U.S. District Court for the Eastern District of New York.

Ropes & Gray LLP
Prudential Tower, 800 Boylston Street
Boston, MA 02199-3600
USA

Tel: +1 617 951 7428
Email: Kevin.Angle@RopesGray.com
URL: www.ropesgray.com

Ropes & Gray is a preeminent global law firm with approximately 1,400 lawyers and legal professionals serving clients in major centers of business, finance, technology and government. The firm has offices in New York, Boston, Washington, D.C., Chicago, San Francisco, Silicon Valley, London, Hong Kong, Shanghai, Tokyo and Seoul, and has consistently been recognised for its leading practices in many areas, including privacy & cybersecurity, private equity, M&A, finance, asset management, real estate, tax, antitrust, life sciences, healthcare, intellectual property, litigation & enforcement, and business restructuring.

www.ropesgray.com

ROPES & GRAY

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: glg global legal group