2024 ASIA-PACIFIC ANNUAL MEETING

9-10 May | The Westin Singapore

ACC Association of Corporate Counsel

in partnership with LEXOLOGY

ACC Association of Corporate Counsel

in partnership with LEXOLOGY

9-10 May | The Westin Singapore

2024 ASIA-PACIFIC ANNUAL MEETING

Exploring Cybersecurity Breaches: What to do in a Disaster?

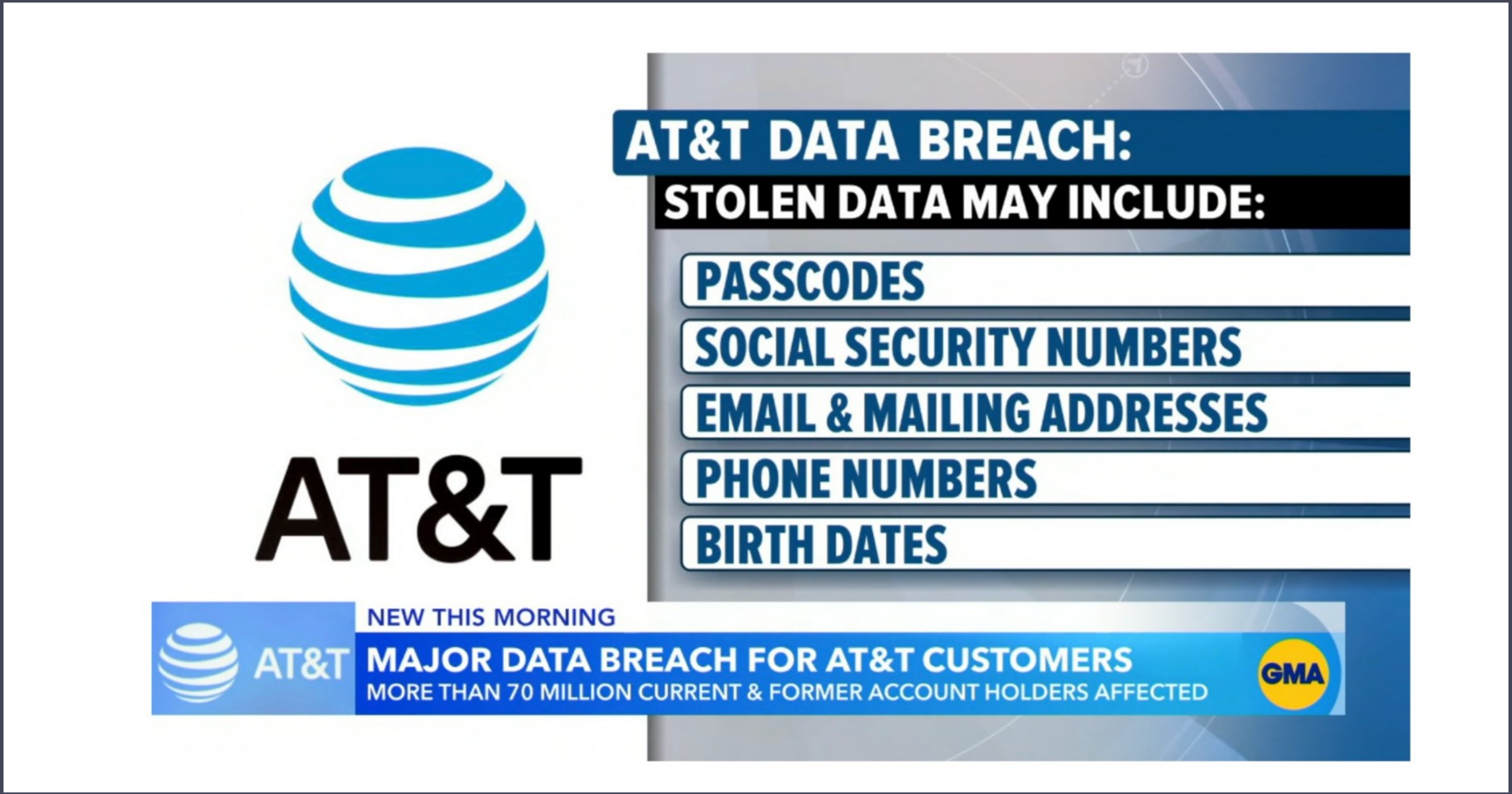
Thamali Tennakoon
Head of Legal
Pyramid Wilmar Pvt Ltd

Christopher . Chan
General Counsel, APAC
Jones Lang LaSalle Inc.

Wilson Tan
Lead Counsel - Global Logistics
Toll Group

Exploring Cybersecurity Breaches: What to do in a Disaster?

Workshop	**Setting the Scene**
	Types of Breaches
	Consequences
	Case study -Anatomy of a RansomWare Attack
	Table Top Scenarios
	How to handle a disaster?
	Q & A



AT&T DATA BREACH:

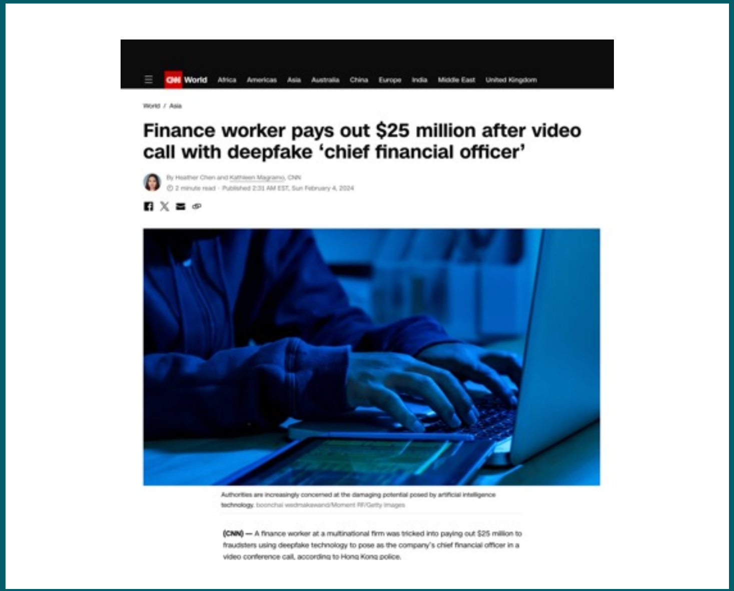
STOLEN DATA MAY INCLUDE:

- PASSCODES
- SOCIAL SECURITY NUMBERS
- EMAIL & MAILING ADDRESSES
- PHONE NUMBERS
- BIRTH DATES

NEW THIS MORNING

MAJOR DATA BREACH FOR AT&T CUSTOMERS

MORE THAN 70 MILLION CURRENT & FORMER ACCOUNT HOLDERS AFFECTED


☰ CNN World Africa Americas Asia Australia China Europe India Middle East United Kingdom

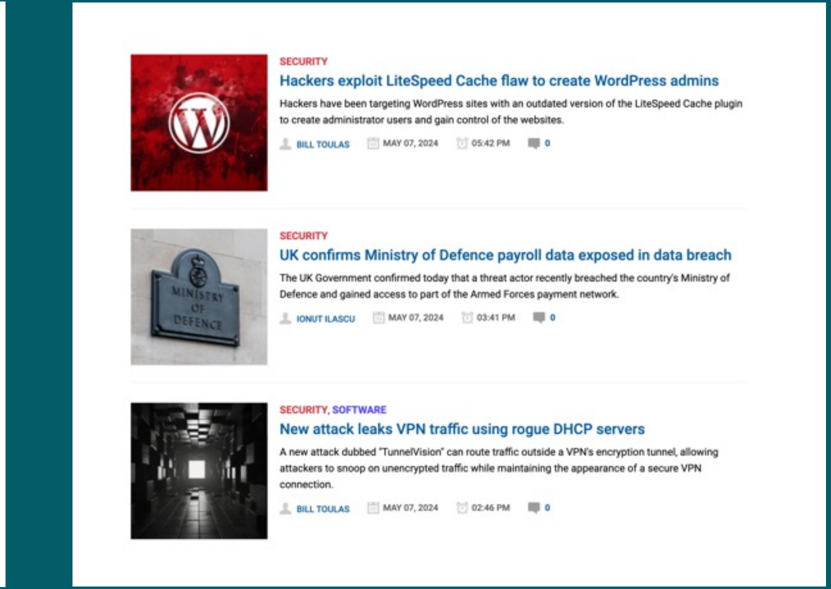
World / Asia

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN
2 minute read · Published 2:31 AM EST, Sun February 4, 2024

Authorities are increasingly concerned at the damaging potential posed by artificial intelligence technology. boonchai wedmakawand/Moment RF/Getty Images

(CNN) — A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call, according to Hong Kong police.


SECURITY

Hackers exploit LiteSpeed Cache flaw to create WordPress admins

Hackers have been targeting WordPress sites with an outdated version of the LiteSpeed Cache plugin to create administrator users and gain control of the websites.

BILL TOULAS · MAY 07, 2024 · 05:42 PM · 0

SECURITY

UK confirms Ministry of Defence payroll data exposed in data breach

The UK Government confirmed today that a threat actor recently breached the country's Ministry of Defence and gained access to part of the Armed Forces payment network.

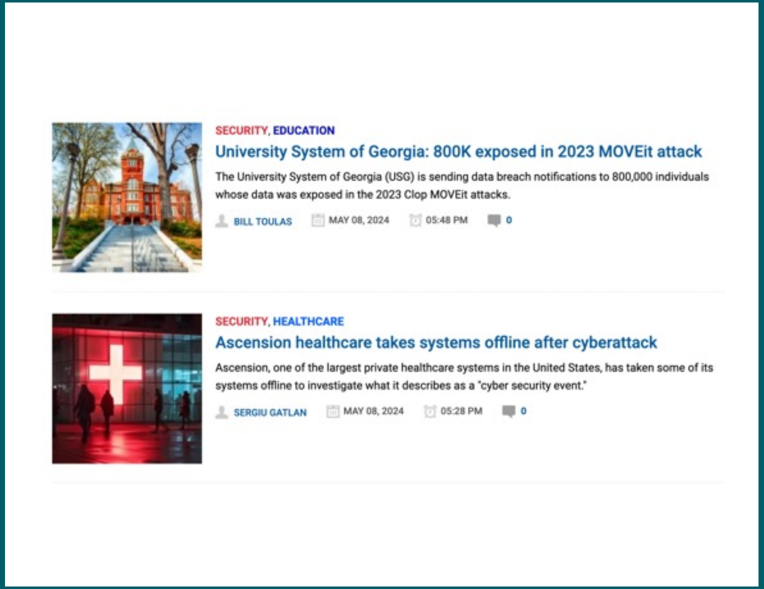
IONUT ILASCU · MAY 07, 2024 · 03:41 PM · 0

SECURITY, SOFTWARE

New attack leaks VPN traffic using rogue DHCP servers

A new attack dubbed "TunnelVision" can route traffic outside a VPN's encryption tunnel, allowing attackers to snoop on unencrypted traffic while maintaining the appearance of a secure VPN connection.

BILL TOULAS · MAY 07, 2024 · 02:46 PM · 0


SECURITY, EDUCATION

University System of Georgia: 800K exposed in 2023 MOVEit attack

The University System of Georgia (USG) is sending data breach notifications to 800,000 individuals whose data was exposed in the 2023 Clop MOVEit attacks.

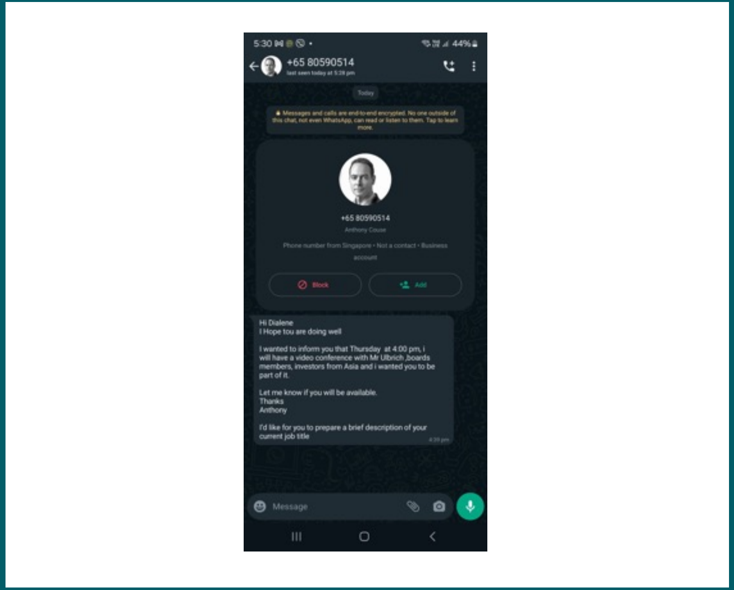
BILL TOULAS · MAY 08, 2024 · 05:48 PM · 0

SECURITY, HEALTHCARE

Ascension healthcare takes systems offline after cyberattack

Ascension, one of the largest private healthcare systems in the United States, has taken some of its systems offline to investigate what it describes as a "cyber security event."

SERGIU GATLAN · MAY 08, 2024 · 05:28 PM · 0


5:30 · 44%
+65 80590514
last seen today at 5:28 pm
Today
Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.
+65 80590514
Anthony Couse
Phone number from Singapore • Not a contact • Business account
Block
Add
Message

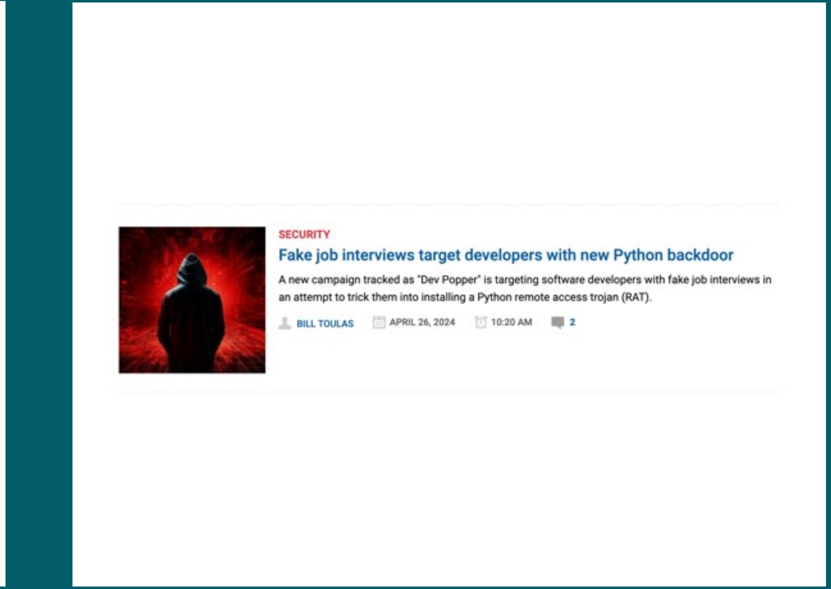
Hi Dialene
I Hope tou are doing well

I wanted to inform you that Thursday at 4:00 pm, i will have a video conference with Mr Ulbrich ,boards members, investors from Asia and i wanted you to be part of it.

Let me know if you will be available.
Thanks
Anthony

I'd like for you to prepare a brief description of your current job title

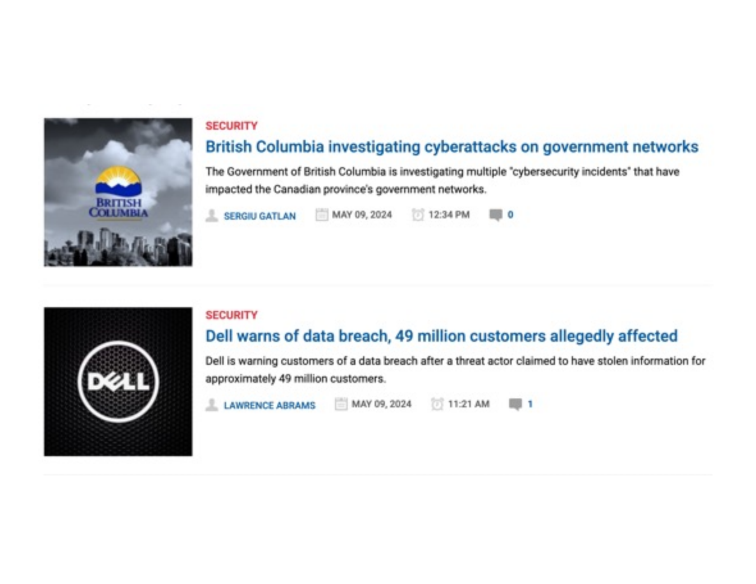
4:39 pm


SECURITY

Fake job interviews target developers with new Python backdoor

A new campaign tracked as "Dev Popper" is targeting software developers with fake job interviews in an attempt to trick them into installing a Python remote access trojan (RAT).

BILL TOULAS · APRIL 26, 2024 · 10:20 AM · 2


SECURITY

British Columbia investigating cyberattacks on government networks

The Government of British Columbia is investigating multiple "cybersecurity incidents" that have impacted the Canadian province's government networks.

SERGIU GATLAN · MAY 09, 2024 · 12:34 PM · 0

SECURITY

Dell warns of data breach, 49 million customers allegedly affected

Dell is warning customers of a data breach after a threat actor claimed to have stolen information for approximately 49 million customers.

LAWRENCE ABRAMS · MAY 09, 2024 · 11:21 AM · 1

Cybersecurity v. Data Privacy

Comprehensive strategies and practices designed to protect an organization's digital assets, systems, and data from cyber threats.

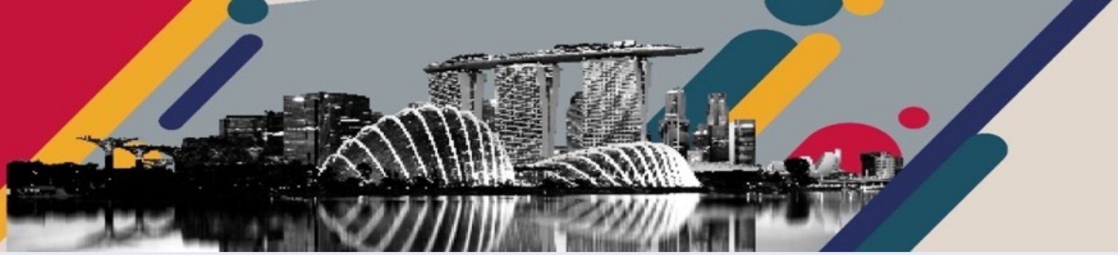
Focus on safeguarding individuals' personal information collected by organizations.

Major Types of Cybersecurity Breaches

- Phishing Attacks – Fake Gmail Logins
- Insider Threat – Edward Snowden
- Ransomware / Malware Attacks - WannaCry
- Supply Chain Attacks - Solarwinds
- Unauthorized Access – JP Morgan Chase
- Internet-of-Things (IoT) Attacks – Mirai BotNet
- DNS Tunneling – Exfiltrate from Network

Consequences of Cybersecurity Breaches

- $$$ Financial Losses
- Reputational Damages
- Legal & Regulatory Consequences
- Violation of IP Rights
- Increased Insurance Costs
- Competitive Disadvantages
- Recoveries Cost and Time



Scenario 1: Phishing Attack

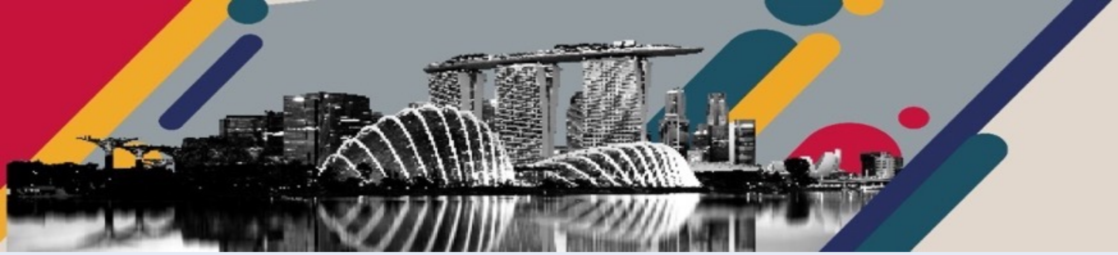
1. Jane - Employee
2. David - Cybersecurity Analyst
3. Sarah - Legal Counsel
4. Michael - IT Administrator

Facts:

•Jane receives **an email disguised as a legitimate message from a known vendor**.
•The **email prompts her to click on a link**, leading to a phishing website.
•Jane **unintentionally provides her login credentials**, enabling the attacker to gain unauthorized access to the company's network.

Key Information:

1.What immediate steps should be taken upon discovering the breach?
2.How should the incident response team proceed to contain the breach?
3.What evidence preservation measures should be considered?
4.What legal obligations and potential liabilities does the company face?
5.How can the company improve employee awareness and training on phishing attacks?



Scenario 2: Supply Chain Attack

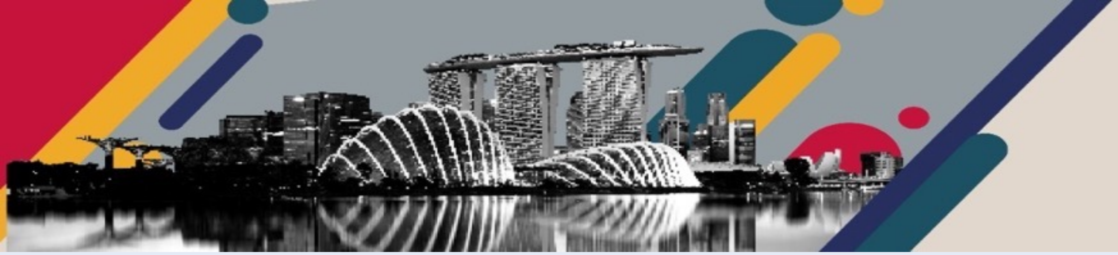
1. Sarah - Legal Counsel
2. Emily - Procurement Manager
3. Patrick - IT Administrator

Facts:

- The company's third-party software vendor experiences a security breach.
- The vendor's compromised software leads to unauthorized access to the company's network.
- The attackers gain access to sensitive customer information.

Key Information:

1. What legal responsibilities does the company have regarding supply chain attacks?
2. How can the organization ensure due diligence and proper vendor management?
3. What contractual safeguards should be put in place to mitigate supply chain risks?
4. How should the organization communicate with affected customers?
5. What steps should be taken to restore trust and prevent future supply chain attacks?



Scenario 3: Insider Threat - Theft by Insider

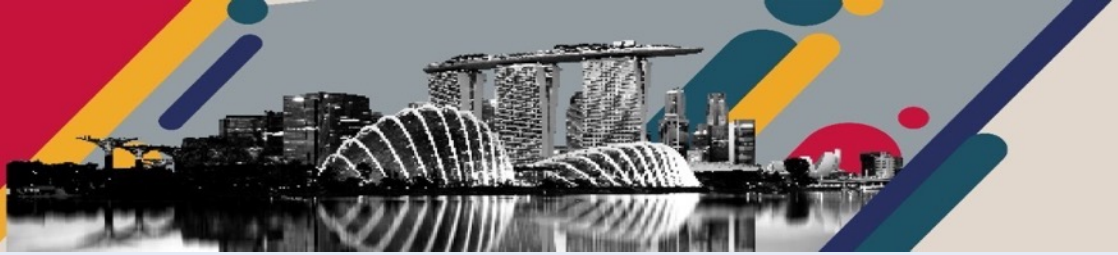
1. Mark - Disgruntled Employee
2. Lisa - Manager
3. Emily - Legal Counsel

Facts:

- Mark, a trusted employee, plans to leave the organization and wants to take valuable customer data with him.
- He uses his access privileges to download sensitive information onto an external device.
- The company's monitoring systems detect Mark's unusual activities.

Key Information:

1. How can the organization detect and mitigate insider threats?
2. What legal actions can be taken to prevent data theft and protect the organization's interests?
3. What role should the incident response team play in managing insider threats?
4. What measures could the company implement to prevent similar incidents in the future?
5. How should the company address employee morale and trust issues after such an incident?



Handling Disasters

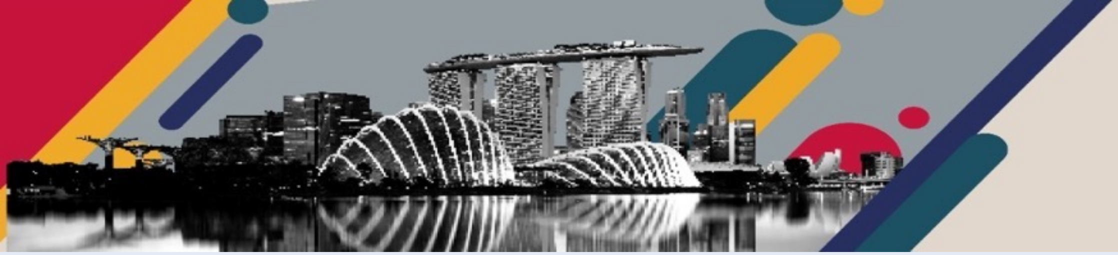
Scenario 1: Phishing Attack

1. **Immediate Steps Upon Discovering the Breach**:

- ✓ Isolate the Affected System: As soon as the breach is detected, disconnect the compromised system from the network to prevent further damage.
- ✓ Change Credentials: Reset Jane’s login credentials immediately to prevent unauthorized access.
- ✓ Notify Incident Response Team (IRT): Inform the IRT, which includes David (the cybersecurity analyst) and Michael (the IT administrator), about the breach.

2. **Incident Response Team Actions**:

- ✓ Assessment: The IRT should assess the extent of the breach, including identifying affected systems, users, and data.
- ✓ Containment: Isolate the compromised system and prevent lateral movement within the network.
- ✓ Eradication: Remove the attacker’s presence from the network by cleaning infected systems.
- ✓ Recovery: Restore affected systems from backups or other secure sources.
- ✓ Lessons Learned: Conduct a post-incident review to learn from the breach and improve security measures.



Handling Disasters

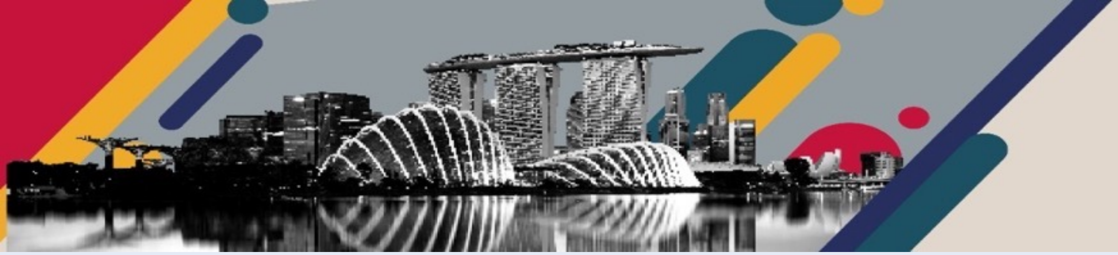
Scenario 1: Phishing Attack

3. Evidence Preservation Measures:

- ✓ Logs: Preserve relevant logs (e.g., email server logs, firewall logs) for forensic analysis.
- ✓ Memory Dump: Capture memory dumps from affected systems.
- ✓ Network Traffic: Analyze network traffic logs to trace the attacker's activities.
- ✓ Chain of Custody: Maintain a proper chain of custody for evidence.

4. **Legal Obligations and Liabilities:**

- ✓ Data Breach Notification Laws: Depending on the company's location, there may be legal requirements to notify affected individuals and regulatory authorities.
- ✓ Contractual Obligations: Review contracts with vendors and assess any liability related to the breach.
- ✓ Potential Fines: Violations of data protection laws can result in significant fines.



Handling Disasters

Scenario 1: Phishing Attack

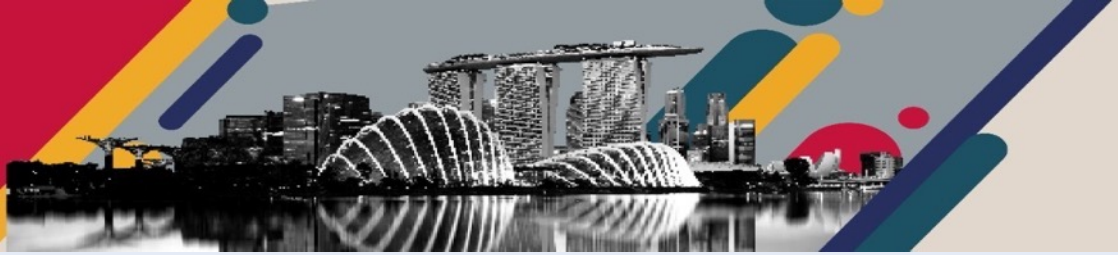
5. Employee Awareness and Training:

✓ Regular Training: Conduct regular security awareness training for employees, emphasizing phishing risks. Simulated Phishing Exercises: Test employees' ability to recognize phishing emails through simulated exercises.

✓ Reporting Mechanisms: Encourage employees to report suspicious emails promptly.

.

Remember that swift action and collaboration among the incident response team, legal counsel, and IT administrators are crucial in mitigating the impact of a phishing attack



Legal Support in a Cybersecurity Breach

Communications to External Stakeholders

1. Media Statements

2. Customer Updates

3. Regulatory Authorities
   a. Personal Data Privacy Commission
   where international personal data involved, obligation to report to national PD agencies
   b. Cyber Security Agency
   providers of critical infrastructure

4. Cybersecurity Insurers

Legal Support in a Cybersecurity Breach

Support to Internal Stakeholders

Legal clearance of situation updates before release

Designated Approved IT Expert(s) to conduct technical briefings with customers & authorities

Customer Notification Obligations

For suspected or actual data privacy breach
For suspected or actual breach of confidential information
For suspected or actual production/service disruptions

Is Cybersecurity Breach a Force Majeure event?

What are Company's obligations if it were to call a Force Majeure event?
Can Company elect to suspend production/services?
Does Customer have step-in rights in a situation of a production/service disruption?
May Customer terminate the contract (in part or in full) for disruption?
Is Company's liability limited or excluded in a cybersecurity breach?

Scenario 1: Phishing Attack

1. Immediate Steps:
    1. Disconnect Jane's device from the network to prevent further unauthorized access.
    2. Document any relevant details about the phishing email for investigation purposes.
    3. Notify the incident response team and escalate the issue to the cybersecurity analyst.
2. Incident Response and Containment:
    1. Conduct a thorough investigation to determine the extent of the breach and identify affected systems or data.
    2. Change Jane's compromised credentials and conduct a review of her account activity.
    3. Communicate with the IT team to implement necessary security measures, such as deploying anti-phishing software.
3. Evidence Preservation:
    1. Collect any available logs, email headers, or other evidence that may assist in identifying the attacker.
    2. Follow proper chain of custody procedures to ensure the collected evidence maintains its integrity.
4. Legal Obligations and Liabilities:
    1. Assess whether any personal data or sensitive information was accessed or compromised.
    2. Determine the need for complying with applicable data breach notification laws and regulations.
    3. Consult with legal counsel to evaluate potential legal liabilities and develop an appropriate response plan.
5. Improving Employee Awareness and Training:
    1. Provide targeted phishing awareness training to all employees, emphasizing the importance of vigilance and best practices.
    2. Implement regular simulated phishing tests to gauge employee response and reinforce training efforts.
    3. Foster a culture of reporting suspected phishing attempts to the IT or security team.

Scenario 2: Insider Threat

1. Detecting and Mitigating Insider Threats:
    1. Implement robust access controls, including the principle of least privilege, to limit employees' access to sensitive data.
    2. Monitor user activities, particularly those involving data downloads or unauthorized access attempts.
    3. Foster a positive work environment with open lines of communication to address employee concerns and discourage malicious intent.
2. Legal Actions and Protection:
    1. Clearly define expectations and obligations related to data protection and confidentiality in employment contracts and policies.
    2. Consider implementing data loss prevention (DLP) solutions to monitor and prevent unauthorized data transfers.
    3. Consult with legal counsel to understand any legal remedies available to protect intellectual property or confidential information.
3. Incident Response Team's Role:
    1. In addition to the cybersecurity team, involve HR and legal in the incident response process to address personnel-related issues.
    2. Assess the potential impact on affected individuals and evaluate the need for external notifications or legal actions.
4. Preventing Similar Incidents:
    1. Foster a culture of trust, fairness, and open communication within the organization to address employee grievances.
    2. Regularly review and update access controls and permissions to align with changing roles and responsibilities.
    3. Conduct periodic internal audits to identify potential policy violations or suspicious activities.
5. Employee Morale and Trust:
    1. Implement programs to enhance employee morale, such as recognition initiatives or team-building activities.
    2. Transparently communicate the organization's commitment to data protection and the steps taken to address the incident.
    3. Provide refresher training to reinforce the importance of safeguarding the organization's assets.

Scenario 3: Supply Chain Attack

1. Legal Responsibilities:
    1. Ensure contracts with third-party vendors include clear data security and privacy provisions, outlining their responsibilities in protecting sensitive information.
    2. Conduct due diligence on vendors to assess their cybersecurity practices and risk management processes.
2. Vendor Management:
    1. Develop a vendor risk management program that includes periodic assessments and audits of vendors' security controls.
    2. Establish incident response and notification protocols to guide actions in case of a breach originating from a vendor.
3. Contractual Safeguards:
    1. Include contractual provisions requiring vendors to promptly notify the company of any breach or suspected compromise.
    2. Include provisions allowing for regular security audits or assessments to verify vendors' compliance with cybersecurity requirements.
4. Communication with Affected Customers:
    1. Develop clear communication plans to inform affected customers, while ensuring compliance with data breach reporting requirements.
    2. Provide guidance and support to affected customers regarding steps they can take to protect themselves from potential harm.
5. Strengthening Supply Chain Security:
    1. Promote continuous monitoring and ongoing assessments of vendors' security practices.
    2. Collaborate with industry peers and associations to share best practices and strengthen supply chain security on a broader scale

Q & A
Discussions