

**Baker
McKenzie.**



Cyber Readiness & Resilience: A New World Order in 2024

December 12, 2023



Agenda

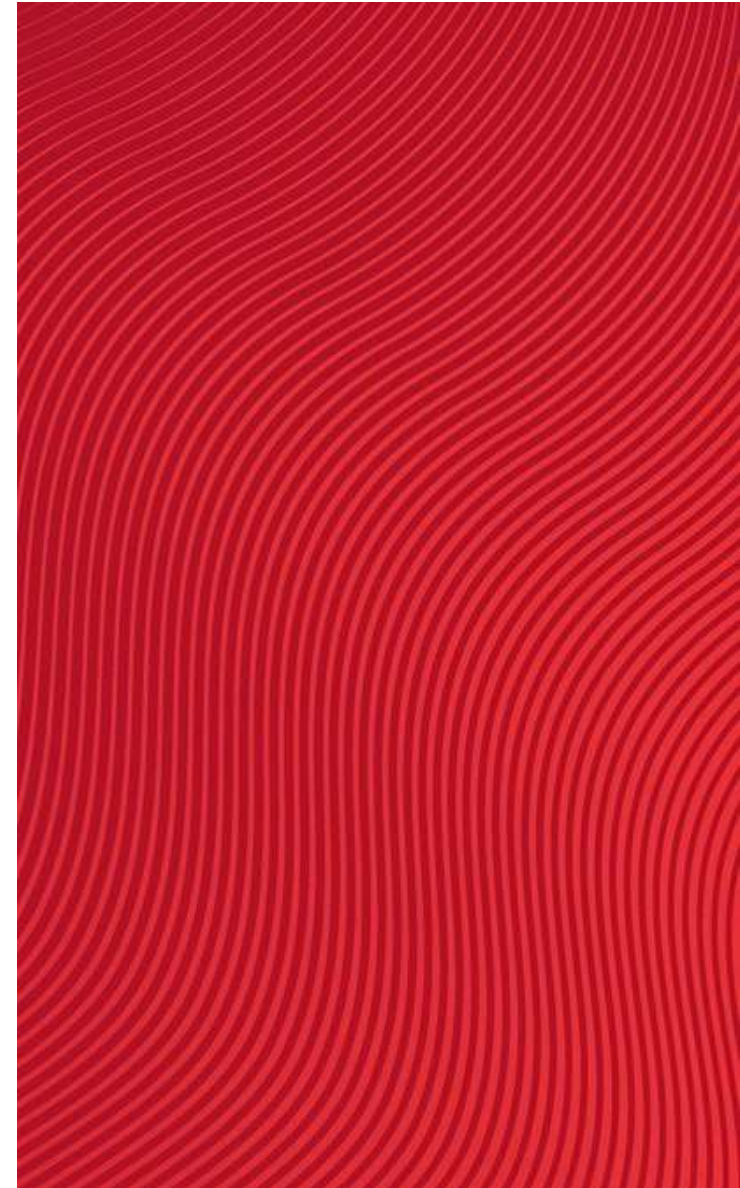
- 01** Current cyber threat landscape

- 02** Key cyber regulations and enforcement actions

- 03** How to evaluate and manage your enterprise cyber risk

- 04** Building a smart, flexible security program leveraging people, process and technology

- 05** Cybersecurity trends to watch in 2024



Hello



Cynthia Cole
Partner
Palo Alto
Baker McKenzie



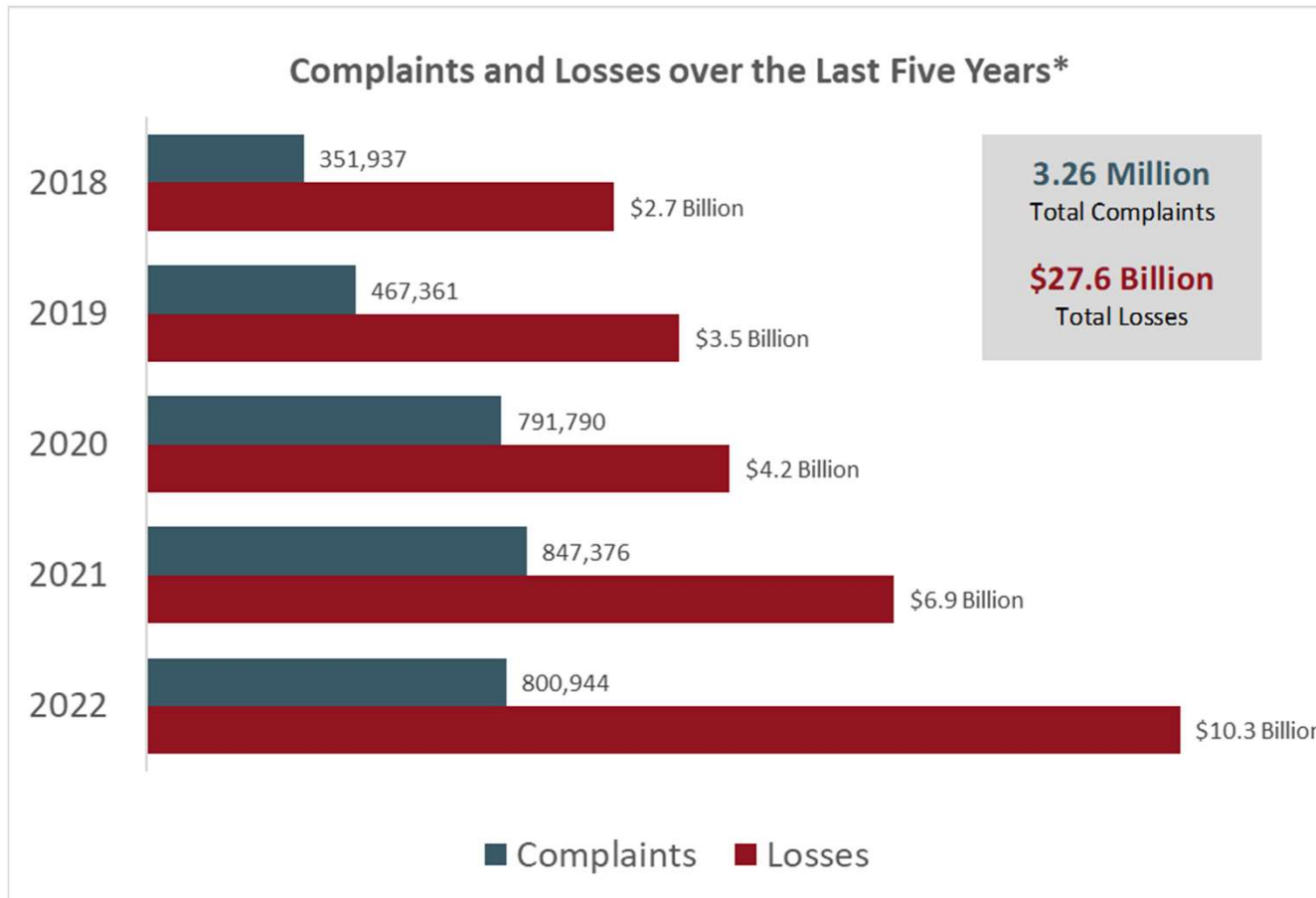
Justine Phillips
Partner
Los Angeles
Baker McKenzie



Jenny Martin
Senior Privacy & Cybersecurity
Counsel
Postman

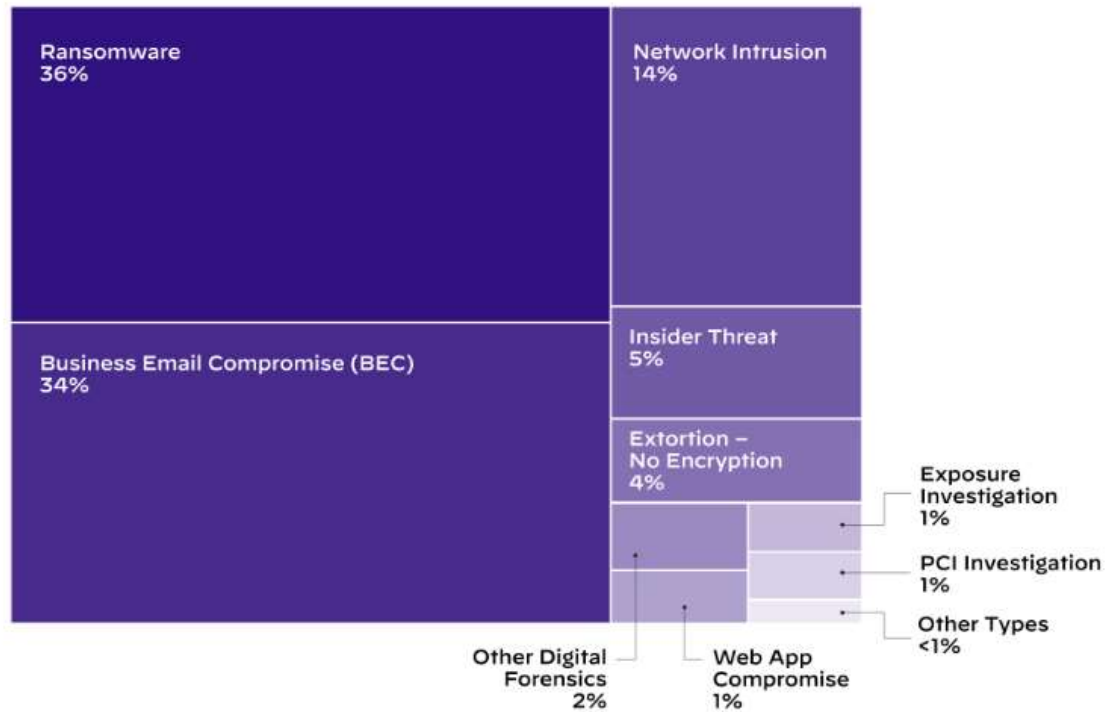
01 Current cyber threat landscape

\$ Cyber Crime Losses \$



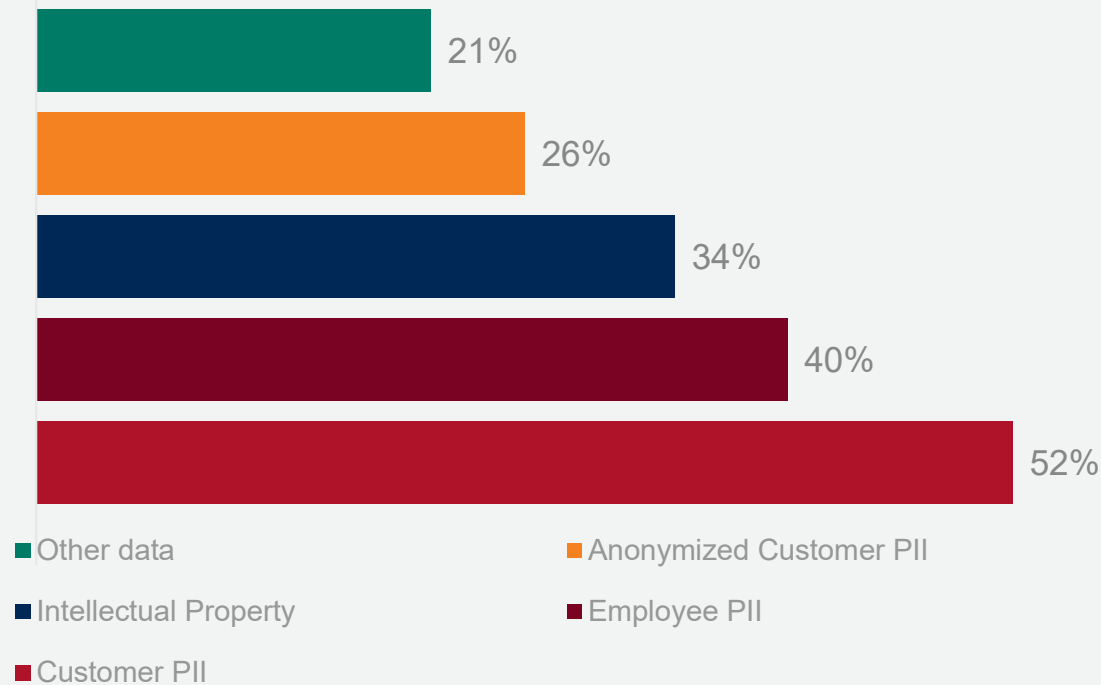
Common Types of Cyber Attacks

Unit 42's 2022 IRT Report



Threat Landscape

Types of data involved in breach



\$9.48 M
*Average total cost
of a US data breach*

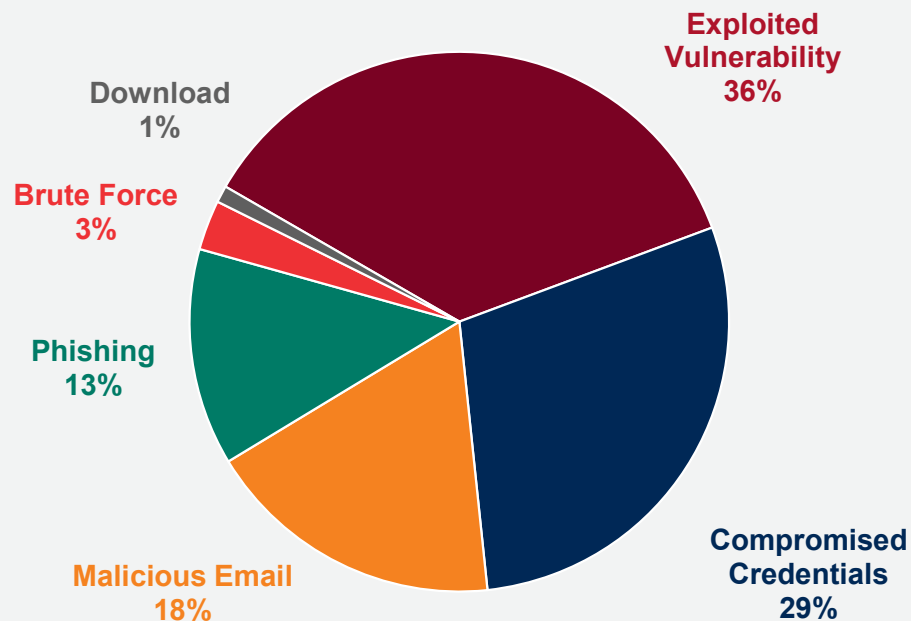
57%
*of data breaches result in
organization increasing the
cost of products or services*

84%
*of private sector organizations hit by
ransomware reported that the attack
caused them to lose revenue*

Sources: IBM – Cost of a Data Breach Report 2023;
Sophos State of Ransomware 2023

Common Attack Vectors

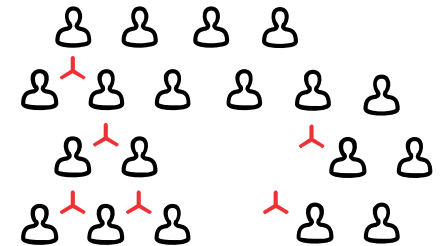
Initial attack vector



Source: Sophos State of Ransomware 2023

74%

of all breaches involve a human element



Source: Verizon Data Breach Investigations Report 2023

According to a 2022 Unit 42 survey:

- In 50% of cases, organizations lacked **multifactor authentication** on key systems
- In 44% of cases, organizations didn't have **endpoint detection and response (EDR) or extended detection and response (XDR)** security
- In 28% of cases, **poor patch management** contributed to attack success
- In 11% of cases, organizations **failed to review/action security alerts**
- In 7% of cases, **weak password security** practices contributed to attack success
- In 7% of cases, **system misconfiguration** was a contributing factor

Current Threat Intelligence: FBI/CISA Advisories

JOINT CYBERSECURITY ADVISORY TLP: CLEAR

Product ID: AA23-075A
March 16, 2023

Coauthored by:



MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

#StopRansomware: LockBit 3.0

SUMMARY

Note: this joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

Actions to take today to mitigate cyber threats from ransomware:

- Prioritize remediating [known exploited vulnerabilities](#).
- Train users to recognize and report [phishing attempts](#).
- Enable and enforce phishing-resistant [multifactor authentication](#).

JOINT CYBERSECURITY ADVISORY TLP: CLEAR

Product ID: AA23-158A
June 7, 2023


#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability

SUMMARY
Updated June 16, 2023

JOINT CYBERSECURITY ADVISORY TLP: CLEAR

Product ID: AA23-320A
November 16, 2023

Co-Authored by:



Scattered Spider

SUMMARY

02 Key cyber regulations and enforcement actions



Critical Infrastructure Risk Management Cybersecurity Improvement Act (CIRCI)



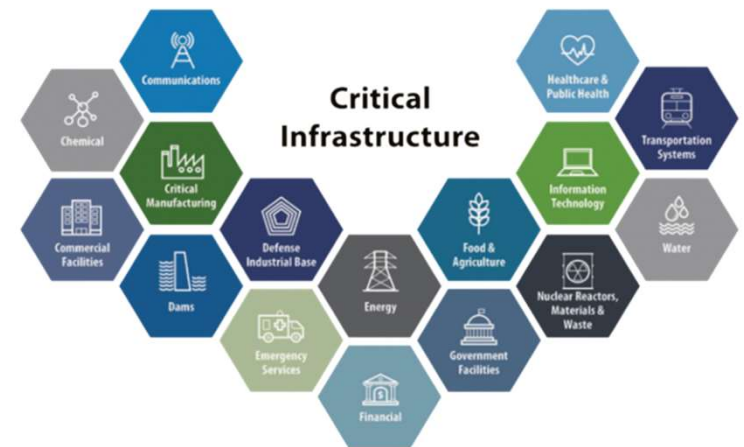
Scope:

- Applies to entities that operate in one of 16 "critical infrastructure sectors" as outlined by Presidential Policy Directive 21 (PPD-21) and who also satisfy the definition of a "covered entity"
- Precise scope subject to forthcoming CISA rulemaking



Key Requirements:

- Report covered cyber incidents within 72 hours of the companies' reasonable belief that a cyber incident has occurred
- Report ransom payments within 24 hours after a payment is made





SEC Rules On Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure

Scope:



- Rules apply to "registrants" (i.e., all public companies that are required to file reports with the SEC, including domestic and foreign issuers)

Key Requirements:



- Make initial determination on materiality of a cybersecurity event "without unreasonable delay"
- If the incident is deemed material, report the incident, using Form 8-K, within four days of the materiality determination (delays only permitted in exceptional circumstances)
- Report annually processes for assessing, identifying, and managing risk from cyber threats, as well as board and management oversight of cyber risks, using Form 10-K (or Form 20-F for foreign issuers)
- Most requirements will come into effect in December 2023



NYDFS Cybersecurity Regulation (23 NYCRR 500)



Scope:

- Entities operating under license, registration, charter, certificate, permit, or accreditation under New York banking, insurance or financial services law



Key Requirements:

- Must maintain and implement cybersecurity program, including:
 - Multifactor authentication
 - Appointment of a CISA
 - Penetration testing and vulnerability assessments
 - Third party provide security policy
 - Limited access privileges
- Notification of within 72 hours of determination that a reportable cybersecurity incident has occurred
- Notification of ransomware payments within 24 hours



California Consumer Privacy Act (CCPA) Cybersecurity Provisions



Scope:

- Applies to for-profit businesses operating in CA that have a gross annual revenue exceeding \$25m and who process the data of at least 100,000 CA consumers annually; or those who derive at least 50% of their revenue from the sale or sharing of personal information
- Establishes limited private right of action for consumers to seek damages from security breaches resulting from a business's violation of the duty to implement and maintain reasonable security procedures and practices



Key Requirements:

- Adopt technical and organizational security measures
- Perform risk assessment prior to conducting certain activities
- Conduct annual cybersecurity audits if processing of consumers' personal information presents significant risk to consumers' privacy or security



Network and Information Security Directive 2 (NIS2)



Scope:

- Applies to organizations that are considered “essential” and “important” entities (NIS2 applies equally to both, but essential entities are subject to stricter enforcement and oversight obligations)
- Categorization depends on entity size and whether entity is in a “critical sector” (waste management, food production) or “very critical sector” (energy, transport)



Key Requirements:

- Adopt technical and organizational security measures
- Ensure their “management bodies” have appropriate oversight and accountability for and training on cybersecurity functions that they manage
- Notify relevant EU state authorities upon learning of a cybersecurity incident (initial notification within 24 hours of becoming aware of incident, with follow up notifications also required)

03 How to evaluate and manage your enterprise cyber risk

Cybersecurity Governance



**Enterprise
Governance**

Corporate Governance

**Stakeholders and
Leadership**

**Cyber Principles &
Organizational Risk Tolerance**

**Policies, IR Plans and
Playbooks**



Implementation

Assessment and categorization of IT tools

Implement technical platforms and inventories

Reporting

Forums, escalations and decision making



**Building
Best practice**

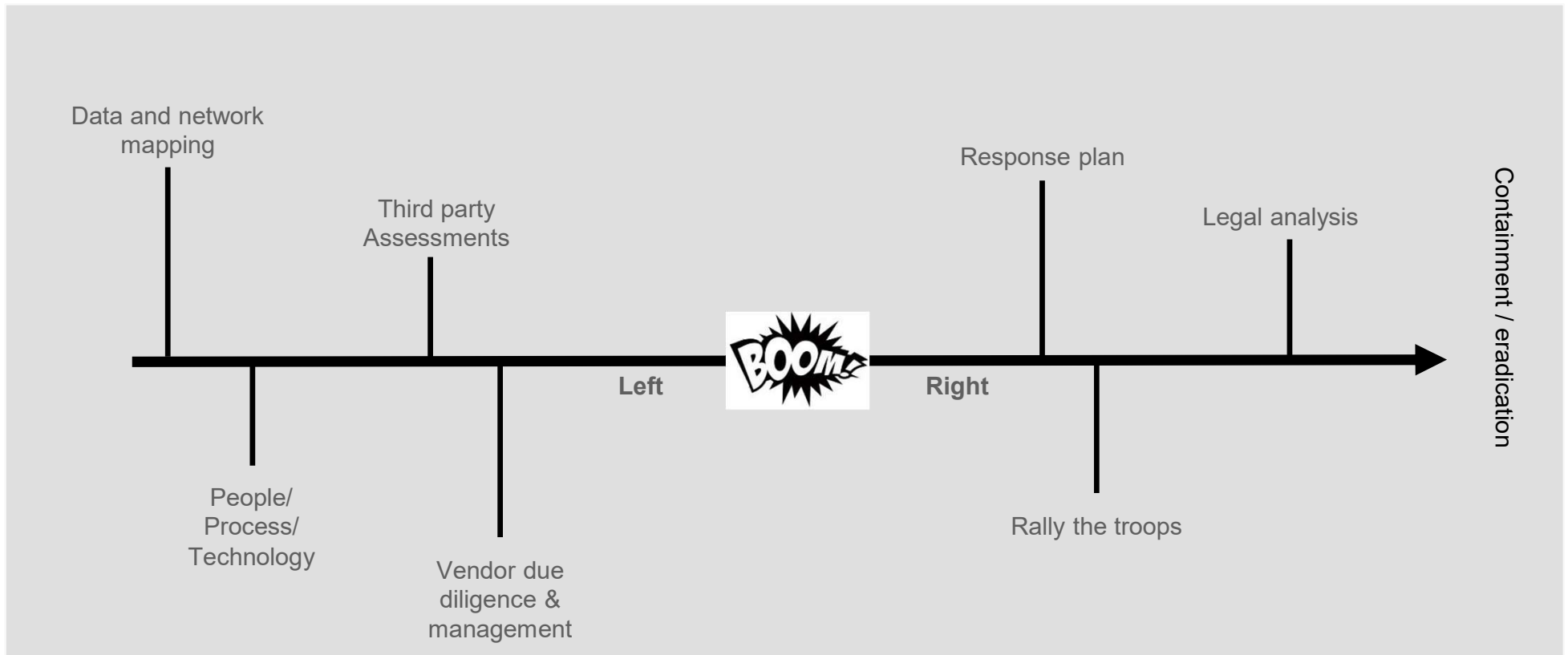
Standards, Processes, Guidance, Templates, Toolkits

Responsible cybersecurity through supply chain (diligence, templates, contract management)

Training and culture

Technical tools and expertise

Proactive vs. Reactive Risk Management



Peoples, Processes, & Tools

Cross-Functional IR Team	
Core Members	Extended Team (incident dependent)
IR Manager	Human Resources
Legal/Privacy	IT Support
CISO/Security Team	Business Continuity
Corp. Communications	Customer Support
Impacted Business Unit	Risk Management
Key External Members	
Outside Counsel	Forensics
Crisis Communications	Investor Relations
Vendors (mail house, call center, credit monitoring)	
Law Enforcement	Insurance Broker



- Processes**
- ✓ Clearly define Roles/Responsibilities (swim lanes)
 - ✓ Clearly defined approval/decision-making authorities
 - ✓ Designate a person to *manage* the end-to-end process (e.g., convene and schedule meetings; track action items; document case file and take notes; manages escalations process)
 - ✓ Regular IRT meetings and status updates
 - ✓ Clear, prompt channels to escalate to Executive Mgmt
 - ✓ Record-keeping

- Tools**
- ✓ Established, direct channels to report suspicious and incidents activity (hotlines, SOC, etc.)
 - ✓ Case management system for record-keeping
 - ✓ Alternative channels of communications
 - ✓ Understand Forensic capabilities, including skills, tools, processes (e.g., chain of custody), geo reach
 - ✓ Current POC lists, including IT support personnel for key system capabilities (e.g., logs, backups, etc.)






Establish relationships between Legal and InfoSec



And be able to articulate how such relationships can help:

- Provides an ally at the senior executive level (GC)
 - Brings in outside counsel for broad experience and perspective on certain issues
 - Provides a legal perspective on the impact side of the risk equation (impact of non-compliance, impact of slow response, etc...)
 - Is a sounding board when contemplating new situations/scenarios
 - Helps with regulatory requests
 - Helps with contract interpretation when dealing with third parties (franchise, vendors)
 - Can be the 'bad cop' when dealing with difficult business partners or third parties
 - Follows changing legislation, keeps us informed, and helps us plan to comply
 - Provides analysis of notification requirements for privacy/security incidents
- 

04 Building a smart, flexible security program leveraging people, process and technology



Cyber Readiness & Resilience: Key Actions

Pre-Attack Readiness: “Left of Boom”

Trainings and Tabletops

Incident Response Plan

Avoidance

- Back-up systems and segregation
- Operational recovery plan
- Back-up communications systems
- Business continuity plan

Engagement with service providers:

- Forensic
- eDiscovery
- PR/Crisis Management
- External legal counsel

Insurance

Post-Attack Response: “Right of Boom”

Containment and info gathering

Systems recovery

Engagement with threat actor

Reporting to authorities and regulators

Dealing with vendors

Breach notification obligations and credit reporting

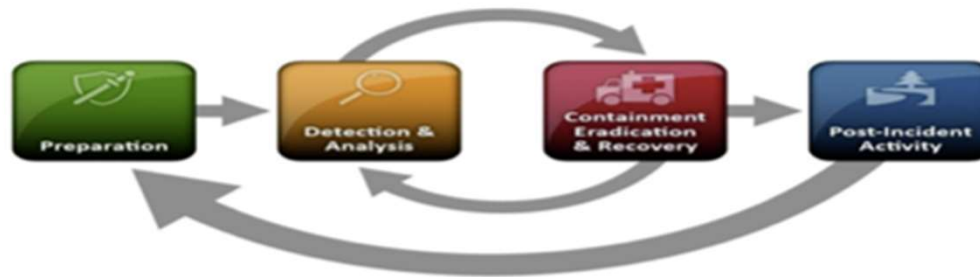
Corporate/employee investigations

Remediation

Litigation and regulatory response

Leveraging Established Guidance, Standards, & Terminology

- ✓ NIST Computer Security Incident Handling Guide (SP 800-61 Rev 2)
- ✓ Use NIST Terminology and ensure consistent terminology between the IRP and internal policies
- ✓ Use NIST Incident Response Lifecycle to frame the IRP:



- ✓ Scope the IRP
- ✓ IRP Maintenance
 - Establish regular table top/simulation exercise schedule
 - Conduct Lessons Learned
 - Review and amend IRP on regular basis

The Response Process



Roles and Responsibilities

Understand which individuals may be called upon during a ransomware incident and delegate roles and responsibilities to them. The identified roles and responsibilities will impact the response process across the entire lifespan of the ransomware incident.

Incident Identification



Trigger IR Plan

- Confirm incident has occurred as defined by Plan
 - Trigger out of band coms
 - Notify IR team of incident
 - Gather data around incident
 - Designate IR commander
- As needed
- Trigger external assistance
 - Connect with law enforcement via counsel

Containment



Run Playbook

- Implement containment strategy to isolate impacted resources and mitigate the spread of attacker across the network.
- Remove and preserve impacted systems before restore
- Validate backup integrity

Investigate



Collect and analyze

- EDR data
 - Log data
 - Forensic Data
 - Intelligence data
- Use data to build timeline
- Use timeline to identify other sources of evidence or other impacted systems

Recovery



Reset and restore

- After investigation clears
- Reset passwords
- Reestablish operations
- Initiate decryption procedures in a testing environment
- Look for opportunities to mitigate future impacts.

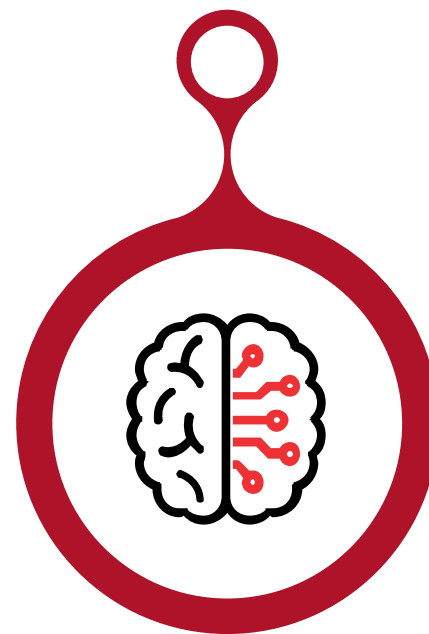
05 Cybersecurity trends to watch in 2024

Key emerging trends

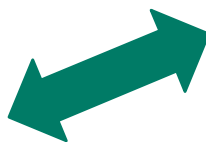
Enforcement
and CISOs



Growing threat actor
sophistication



Disclosures under
the new SEC Rules





Focus on InfoSec Function: SolarWinds

Background & SEC Enforcement



- In Dec 2020, SolarWinds, which provides IT management solutions, disclosed that it had detected that Russian intelligence actors has injected malicious code into its Orion software, which is used by approximately 33,000 customers
- Among those affected were multiple US federal agencies (including the Treasury Department, CDC, DoJ, FAA), NATO, the U.K. government, the European Parliament, Microsoft
- According to a White House briefing, this compromise allowed Russian intelligence "to spy on or potentially disrupt more than 16,000 computer systems worldwide"
- On October 30 the SEC filed a SDNY complaint, naming both SolarWinds and Timothy Brown, its CISO, as defendants and alleging Brown (1) failed to maintain a secure development lifecycle, (2) didn't enforce the use of strong passwords, and (3) didn't remedy access control problems

THE WALL STREET JOURNAL.

Oct. 30, 2023

Cyber Chiefs Worry About Personal Liability as SEC Sues SolarWinds, Executive

Tim Brown, the company's top security executive, is named in SEC suit

As the Securities and Exchange Commission gets more aggressive in enforcing cybersecurity regulations, corporate cyber chiefs want to insulate themselves from potential liability. The SEC on Monday sued technology company SolarWinds and its head of security, alleging they defrauded shareholders by misleading them about cyber vulnerabilities and the scope of a 2020 cyberattack.





SEC Disclosure Considerations



Company may be required to disclose certain data security incidents in SEC filings, or update prior disclosures based on the occurrence of such incidents (e.g., a Form 8-K), in particular where information would be material to an investor's decision -- *SEC Statement and Guidance on Public Company Cybersecurity Disclosures*.



Risk Factors and MD&A in 10-Ks must reflect information on material cyber incidents and material cyber risks presented to its business.



Increasing SEC Enforcement focus on sufficiency of a company's disclosure controls and procedures related to cyber incidents.



The company must also have policies and procedures in place to guard against executives and others from trading on the basis of material non-public information, including knowledge of data security incidents where applicable.

New threat actor tactics



- On Nov 7, ransomware gang BlackCat/ALPHV claimed it had compromised digital lending solutions provider MeridianLink
- After MeridianLink's refusal to engage, Blackcat reported MeridianLink on the SEC's "Tips, Complaints, and Referrals" site

* In your own words, describe the conduct or situation you are complaining about.

We want to bring to your attention a concerning issue regarding MeridianLink's compliance with the recently adopted cybersecurity incident disclosure rules.

It has come to our attention that MeridianLink, in light of a significant breach compromising customer data and operational information, has failed to file the requisite disclosure under Item 1.05 of Form 8-K within the stipulated four business days, as mandated by the new SEC rules.

- Impact on ransomware payments

New threat actor tactics: Use of AI

Malware creation:

- Expediting process of coding new malware
- Creation of new variants to evade attribution by signature detection
- Creation of new variants with new functionalities

Malware delivery:

- Bypassing EDR
- Password guessing
- Generation of malicious ads
- Enhancing phishing and other social engineering vectors
- Enabling social engineering at scale (e.g., through deepfakes, voice and language generation)

BLACKMAMBA: USING AI TO GENERATE POLYMORPHIC MALWARE

Posted by Jeff Sims | July 31 2023



HYAS

But can also be used for prevention, detection & response:

- Threat tracking and intelligence
- Reducing false positives
- Attack containment and system recovery



Baker McKenzie Resources

For more, visit our [Connect on Tech Blog & Podcast Series](#)

Data Privacy, Cyber & California Specific

[First Look at California Privacy Protection Agency's Proposed Regulations on Risk Assessments](#)

[Key Takeaways from CPPA's Public Meeting Discussing Risk Assessments and Cybersecurity Audits](#)

[California Governor Issues Executive Order Addressing the Development of Generative Artificial Intelligence](#)

[How existing data privacy laws may already regulate data-related aspects of AI](#)

Artificial Intelligence

[A landmark week in AI policy developments: what you need to know](#)

[Innovation and Accountability: Asking Better Questions in Implementing Generative AI](#)

[Biden's Wide-Ranging Executive Order on Artificial Intelligence Sets Stage For Regulation, Investment, Oversight and Accountability](#)

[FTC Recommends Transparency When Selling Digital Products and Developing AI Tools](#)

[Check Yourself Before You Wreck Yourself: New York and Other States Have Big Plans For Employer Use of AI and Other Workplace Monitoring Tools](#)

Cybersecurity

[SEC Adopts Final Cybersecurity Rules](#)

[Hacker attempts to use SEC rules to further exploit victims](#)

[New York State Sets the Bar for Cybersecurity Requirements](#)

[CISOs, Internal Accounting Controls, Crown Jewels and Disclosure Procedures: Peeling Back The Onion of the Solar Winds Enforcement Action](#)

[Podcast Episode: The SEC's Final Cybersecurity Rules - A Look at Evolving Risks in the New Age](#)

Welcome to the Global Data Privacy & Security Handbook



[Click to view](#). Will be updated Jan 2024



External Resources

[FBI Guidance to Victims of Cyber Incidents on SEC Reporting Requirements](#)

[Data Privacy And Cybersecurity Issues In Mergers And Acquisitions \(Forbes article\)](#)

[DHS-CISA Updates](#)

Questions