



CHARLESTON
SCHOOL OF LAW

Charleston CyberLaw Forum

January 18, 2024



CHARLESTON
SCHOOL OF LAW

Hacking Incident Response: Pro TTPs Left and Right of Boom

The CLE materials are sponsored by SentinelOne and Charleston Law School. All CLE materials are prepared by law firms and attorneys as noted in the materials, and do not offer any specific legal advice or guidance.

**Baker
McKenzie.**

 **FTI**TM
CONSULTING

**Booz
Allen.**

 **solis**

Presenters



Justine Phillips

Partner
Baker & McKenzie LLP



Nikole Davenport

Senior Managing Director
FTI Consulting



Brendan Rooney

VP, Global Commercial IR
Booz Allen



Terry Oehring

CEO
Solis Security



The Best Friend of Charleston





Presentation Agenda

1

Current Cyber Threat Landscape

2

**Key Cyber Regulations and
Enforcement Actions**

3

**How to Evaluate and Manage
Your Enterprise Cyber Risk**

4

**Building a Smart, Flexible Security
Program Leveraging People,
Process and Technology**

5

Cybersecurity Trends to Watch in 2024



CHARLESTON
SCHOOL OF LAW

01

Wrong Side of the Tracks: Threat Actors and Threat Landscape

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: CLOP Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability

SUMMARY
Updated June 16, 2023

JOINT CYBERSECURITY ADVISORY TLP: CLEAR

Co-Authored by:



Product ID: AA23-320A
November 16, 2023

Scattered Spider

SUMMARY

New TTPs by New Threat Actors

What are
new TTPs
Threat Actors
are using?

1

New attack
vectors?

2

Bypassing
MFA and
XDR tools?

3

What has
changed?

4

How can we
stay up to date
about new
attack vectors
and threats?

5

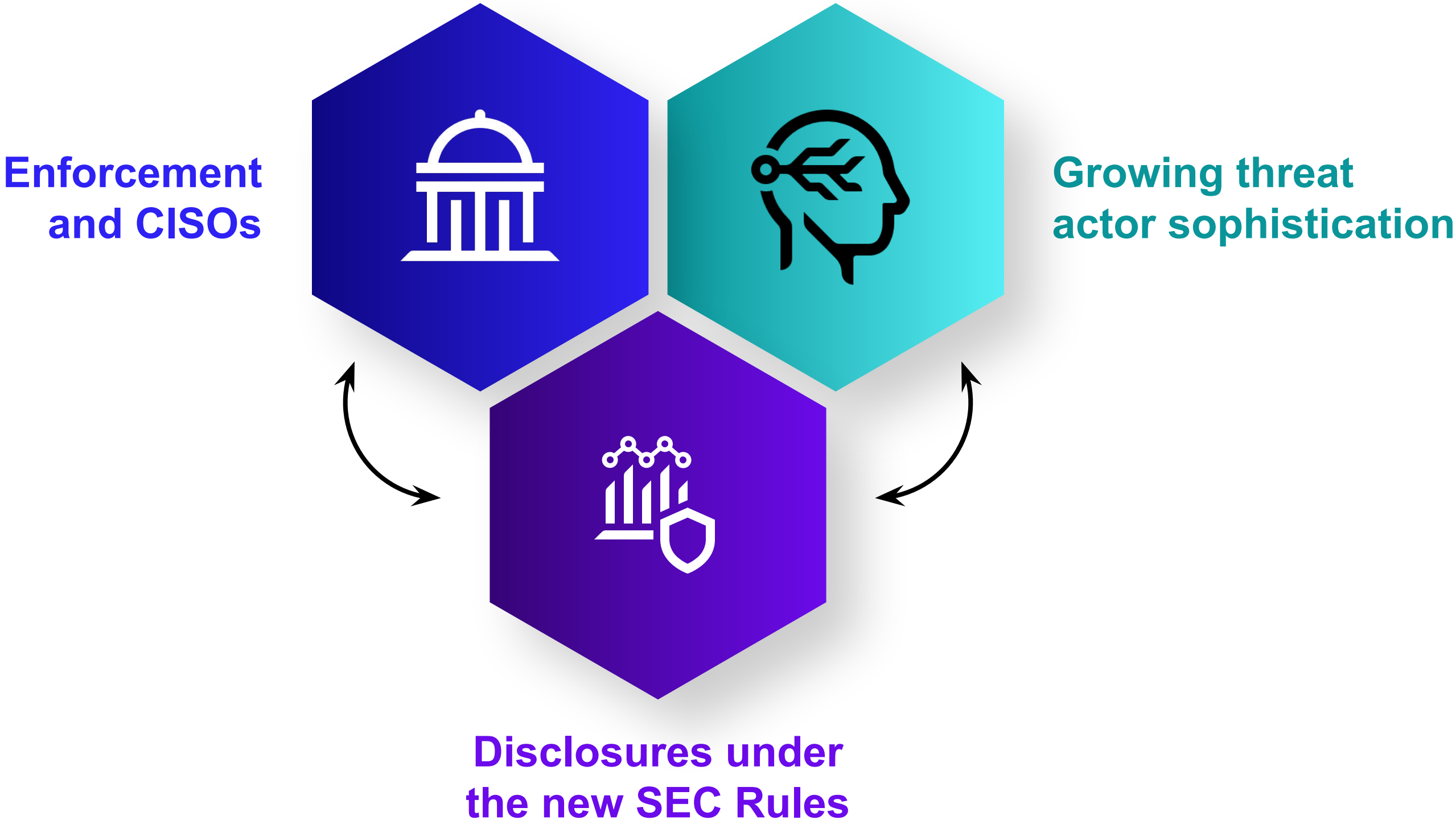


CHARLESTON
SCHOOL OF LAW

02

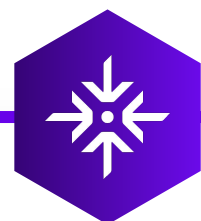
Guard Rails: Key Cyber Regulations and Enforcement Actions

Key Emerging Trends



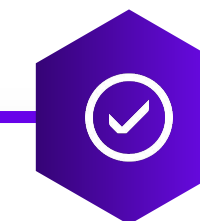


Critical Infrastructure Risk Management Cybersecurity Improvement Act (CIRCI)



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

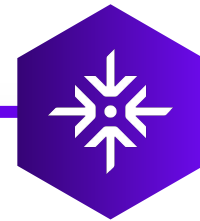


Key Requirements:

- 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

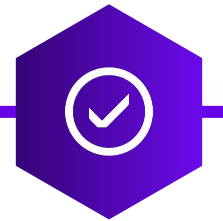


SEC Rules On Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure



Scope:

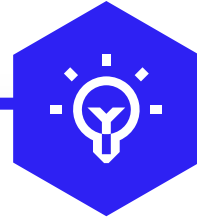
- Rules apply to "registrants" (i.e., all public companies that are required to file reports with the SEC, including domestic and foreign issuers)



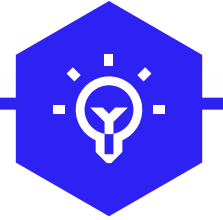
Key Requirements:

- 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 went into effect in mid December 2023
- Proactive (10-K) and reactive (8-K) statements are rolling in

SEC Disclosure Considerations



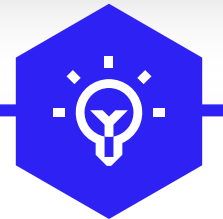
Company may be required to disclose certain data security incidents in SEC filings, or update prior disclosures based on the occurrence of such incidents (e.g., a Form 8-K), in particular where information would be material to an investor's decision -- SEC Statement and Guidance on Public Company Cybersecurity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



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

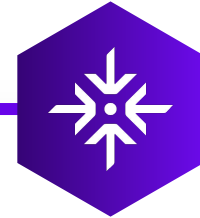


Increasing SEC Enforcement focus on sufficiency of a company's disclosure controls and procedures related to cyber incidents.



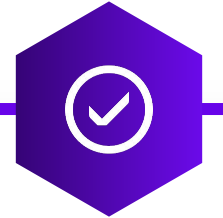
The company must also have policies and procedures in place to guard against executives and others from trading on the basis of material non-public information, including knowledge of data security incidents where applicable.

NYDFS Cybersecurity Regulation (23 NYCRR 500)



Scope:

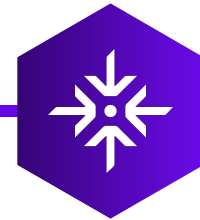
- Entities operating under license, registration, charter, certificate, permit, or accreditation under New York banking, insurance or financial services law



Key Requirements:

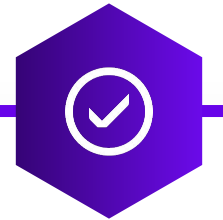
- Must maintain and implement cybersecurity program, including:
 - Multifactor authentication
 - Appointment of a CISA
 - Penetration testing and vulnerability assessments
 - Third party provide security policy
 - Limited access privileges
- Notification of within 72 hours of determination that a reportable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

California Consumer Privacy Act (CCPA) Cybersecurity Provisions



Scope:

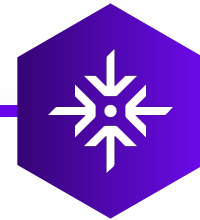
- Applies to for-profit businesses operating in CA that have a gross annual revenue exceeding \$25m and who process the data of at least 100,000 CA consumers annually; or those who derive at least 50% of their revenue from the sale or sharing of personal information
- Establishes limited private right 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:

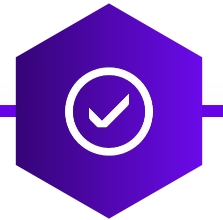
- Adopt technical and organizational security measures
- Perform risk assessment prior to conducting certain activities
- Conduct annual cybersecurity audits if processing of consumers' personal information presents significant risk to consumers' privacy or security
- New regulations expected by March or April 2024

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)

Focus on InfoSec Function: SolarWinds

Background and SEC Enforcement



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.

New TTPs by New Threat Actors

How will these new laws impact our industry?

1

What actions companies are taking now?

2

How have incident response plans changed to comply with these new laws?

3

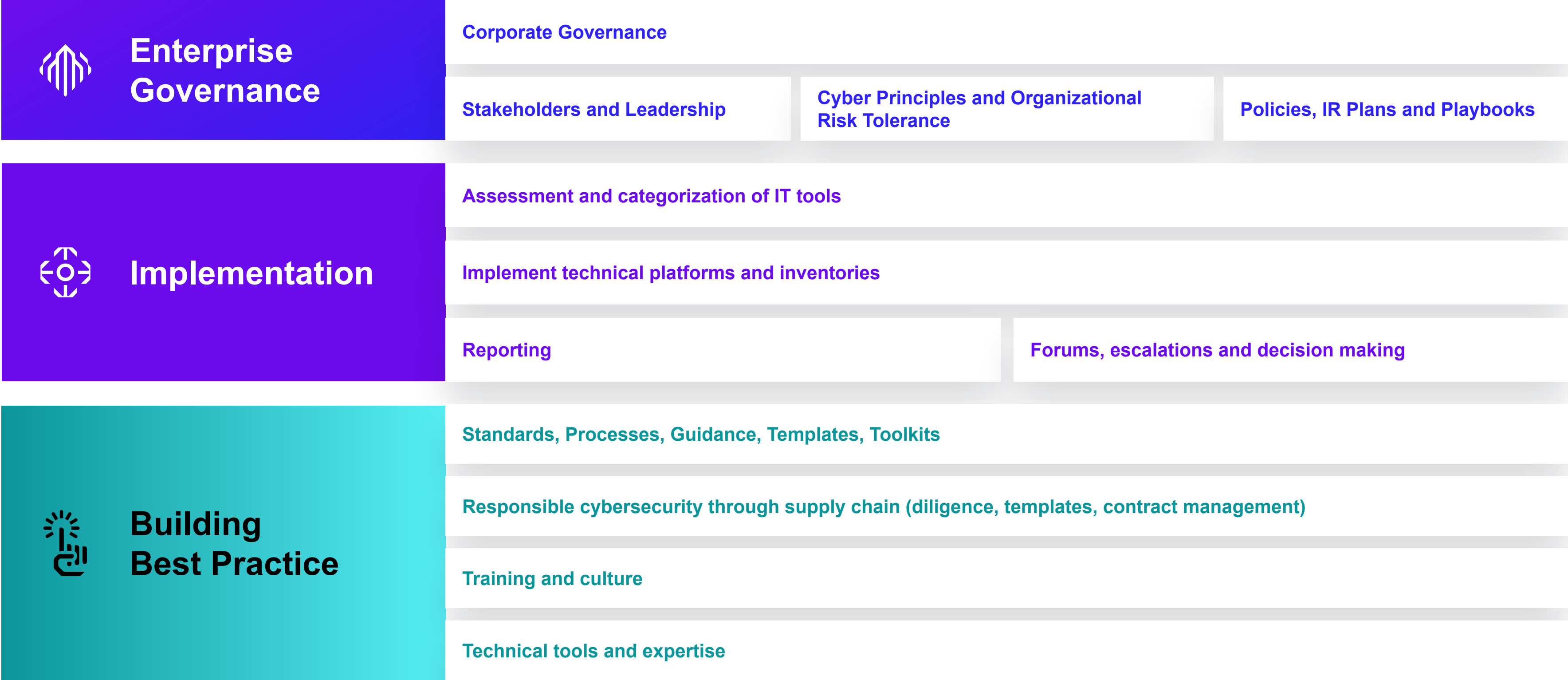


CHARLESTON
SCHOOL OF LAW

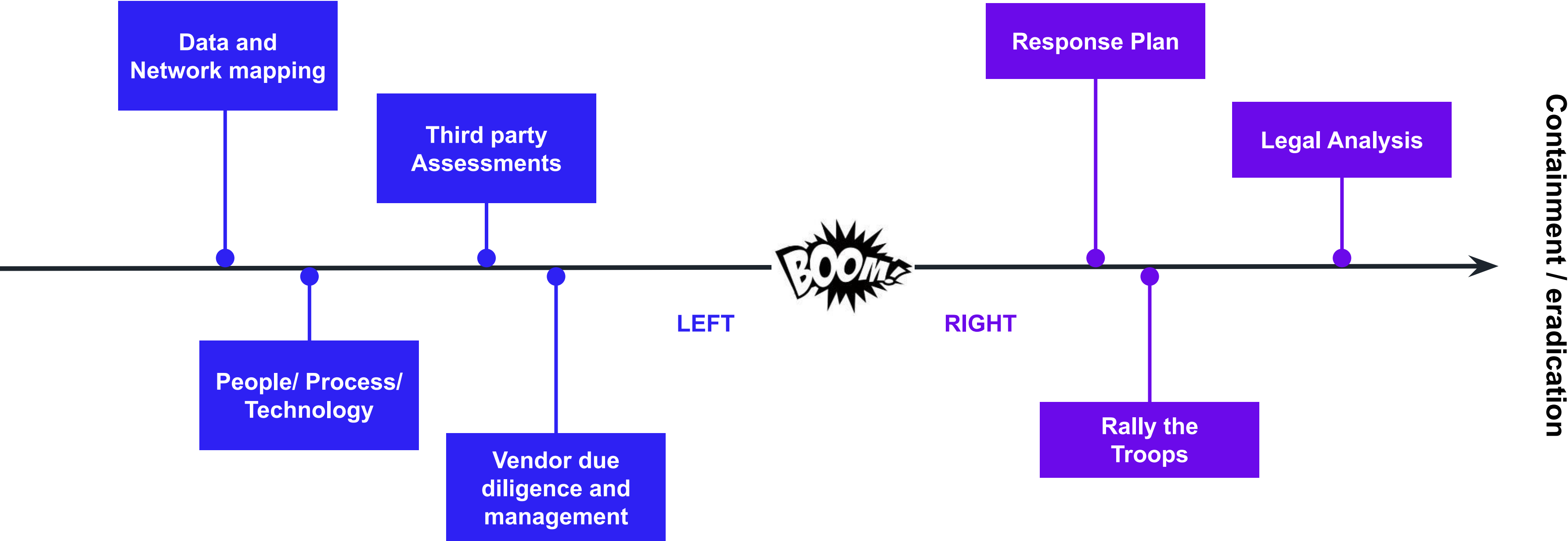
03

The Little Engine That Could: Building an Enterprise Cyber Risk Governance Program

Cybersecurity Risk Governance



Proactive vs. Reactive Risk Management



Cyber Readiness and 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

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

Establish relationships between Legal and InfoSec

What are the TTPs
to mitigating cyber
risk left of boom?

1

How do we effectively
govern cyber risk
when it is constantly
changing?

2

Who are the
cyber allies in
the enterprise?

3



CHARLESTON
SCHOOL OF LAW

04

Off the Rails: Building a Resilient IR Program by Leveraging People, Process and Technology

Cyber Readiness and Resilience: Key Actions

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, and 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 tabletop/simulation exercise schedule
 - Conduct lessons learned
 - Review and amend IRP on regular basis

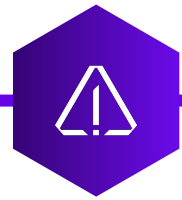
The Response Process



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.

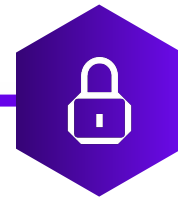
Incident Identification



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

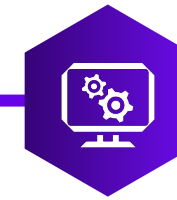
Containment



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

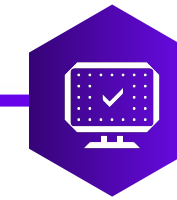
Investigate



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

I Think I Can, I Think I Can

What are the TTPs to mitigating cyber risk left of boom?

1

How do we effectively govern cyber risk when it is constantly changing?

2

Who are the cyber allies in the enterprise? Outside the enterprise?

3

Can DDW Threat Intel help?

4

How can law enforcement support?

5

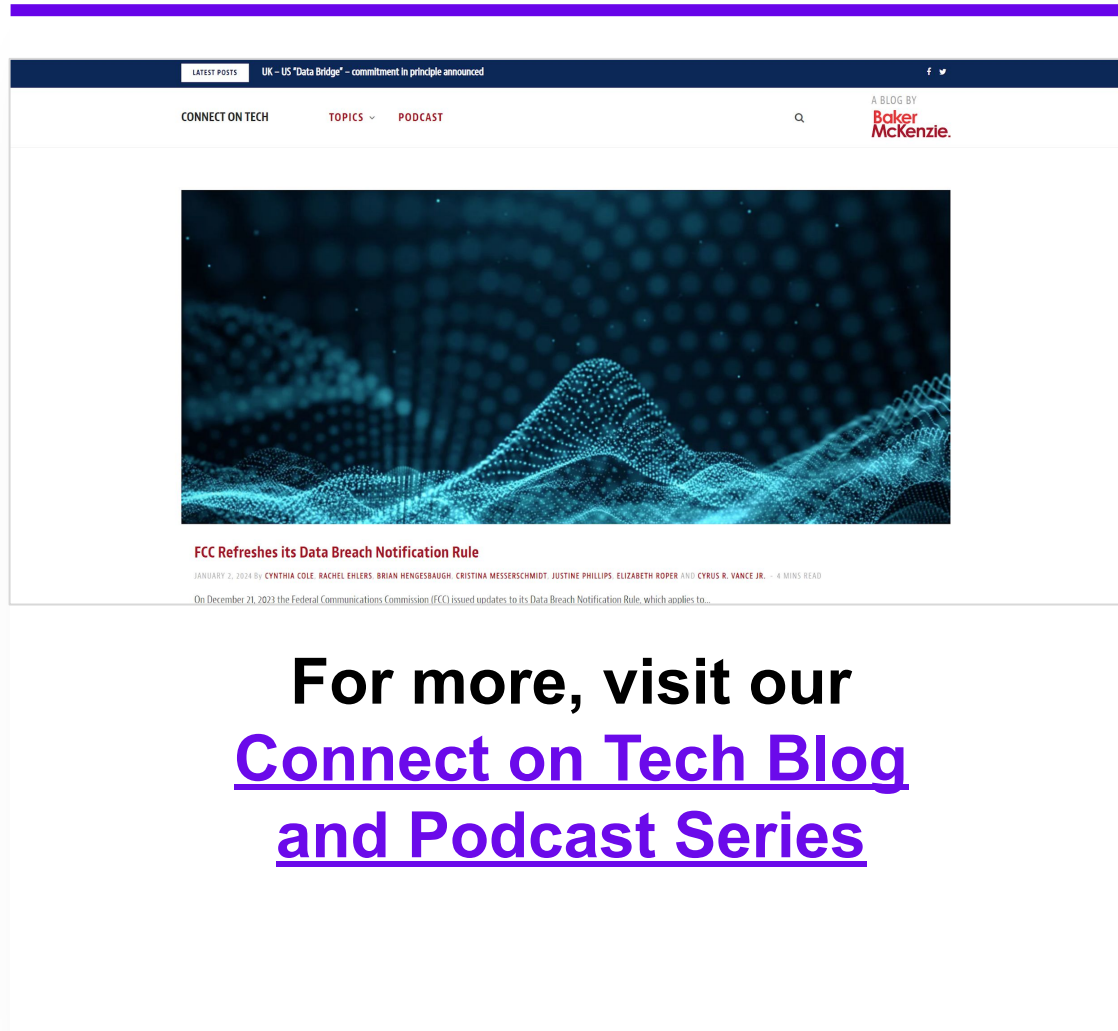


CHARLESTON
SCHOOL OF LAW

Your Roundtrip Ticket: Resources

05

Baker McKenzie Resources



The screenshot shows the Baker McKenzie website's 'Connect on Tech' section. It features a dark blue header with navigation links for 'CONNECT ON TECH', 'TOPICS', and 'PODCAST'. Below the header is a large image of a glowing blue data landscape. A featured article titled 'FCC Refreshes its Data Breach Notification Rule' is visible, with a date of January 2, 2024, and a list of authors including Cynthia Cole, Rachel Ehlers, Brian Hengesbaugh, Cristina Messerschmidt, Justine Phillips, Elizabeth Roper, and Cyrus R. Vance Jr. Below the article is a call to action: 'For more, visit our [Connect on Tech Blog](#) and [Podcast Series](#)'.

**Baker
McKenzie.**

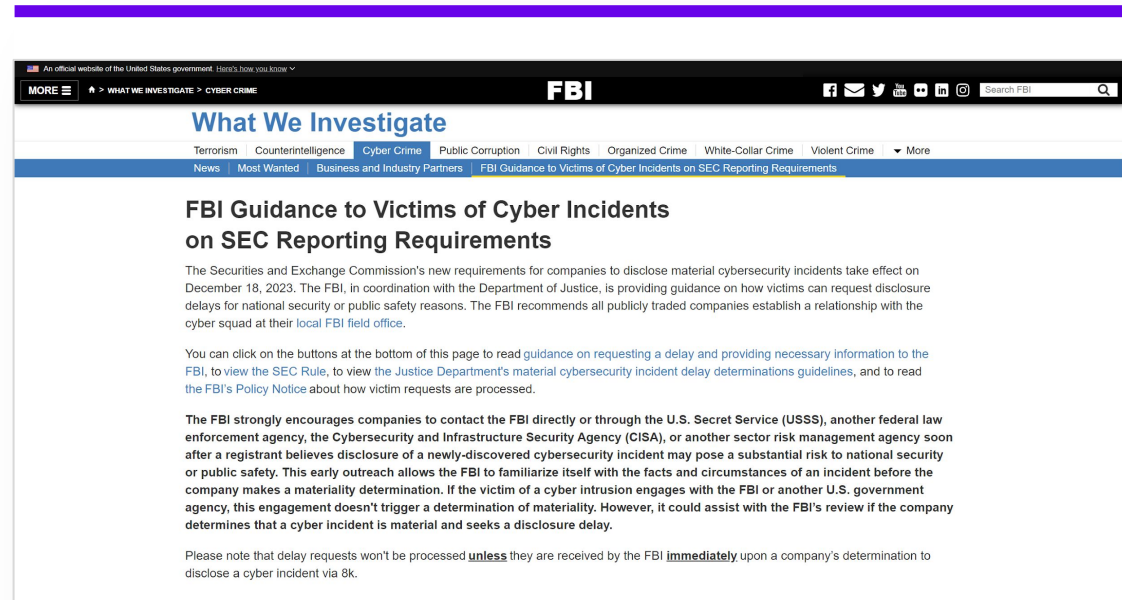
**Welcome to the Global Data Privacy &
Security Handbook**



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](#)
- [Baker McKenzie Global Data Privacy and Security Handbook: Click to view.](#) Will be updated Jan 2024

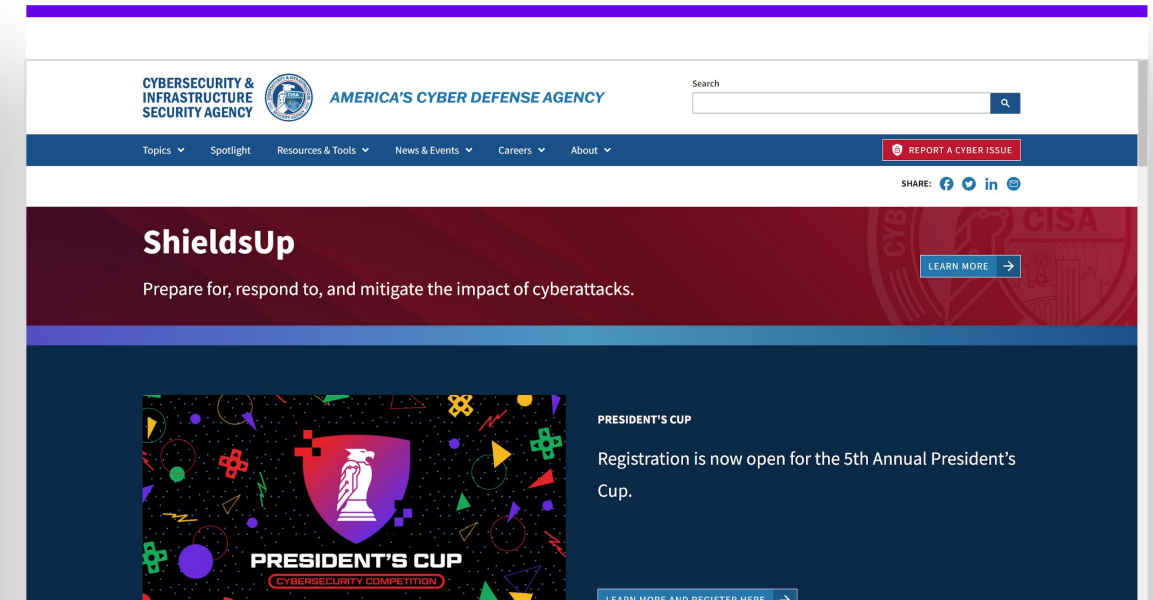
External Resources



[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: https://www.cisa.gov/](https://www.cisa.gov/)



Justine Phillips

Partner, Baker & McKenzie LLP

**Baker
McKenzie.**

Justine focuses her practice on both proactive and reactive cybersecurity and data privacy services, representing clients in matters related to information governance, diligence in acquisitions and investments, incident preparedness and response, the California Consumer Privacy Act, privacy litigation, and cyber litigation.

She provides actionable and practical guidance to help businesses manage data, technology, cyber threats, privacy, security and digital assets. As businesses navigate complex and far-reaching laws and regulations, Justine proactively creates compliance programs customized to client needs and budgets, including data mapping, vendor management, privacy and security by design, cyber risk management and mitigation, eWorkforce policies, data retention and destruction policies and implementation, consumer request workflows, cyber-awareness policies and trainings, and CCPA/CPRA readiness audits. She also provides reactive cyber services, including incident response, crisis management, privileged forensic investigations into business email compromises, data breaches and ransomware attacks, compliance with notice obligations to individuals and regulators, regulatory inquiries and investigations, and cyber litigation. Justine also handles employment litigation and counseling, as well as commercial litigation.

Justine received her law degree from the University of San Diego School of Law (magna cum laude) and her Bachelor of Arts from the University of San Diego.



Nikole Davenport

Senior Managing Director, FTI Consulting



Nikole Davenport is a regulatory compliance expert with more than 20 years of experience in information security focused on data compliance. Ms. Davenport specializes in developing data compliance programs that protect personal data from problem identification through implemented solutions.

Ms. Davenport came to FTI from Meta, where she served as the Head of Regulatory Readiness and Response Programs for WhatsApp. In this role, she led a team of experts to deliver strong programmatic execution for global data compliance, including information security, content and integrity and business regulatory strategy for WhatsApp. She assessed geographic and intra-company contagion risks and created readiness and response strategies to align the interests of product, policy, legal, engineering and marketing segments.

Prior to her tenure at Meta, Ms. Davenport held the position of Chief Privacy Officer and Vice President of Privacy Programs at HITRUST Alliance. She also previously served as a Senior Manager of Cyber Risk and Data Privacy at Deloitte, and as a Law Partner at Chitwood Harley Harnes, LLP.

Ms. Davenport holds her LL.M. from Emory Law and a J.D. from Temple University School of Law. She is a member of the Georgia Bar Association and is Certified Information Privacy Professional (“CIPP”), Certified Information Privacy Manager (“CIPM”), Fellow of Information Privacy (“FIP”), and Certified Data Privacy Solutions Engineer (“CDPSE”) certified.



Brendan Rooney

Vice President, Global Commercial Incident Response, Booz Allen

**Booz
Allen**

Brendan brings a diverse background in cyber risk, drawing upon prior roles in the cyber insurance and cybersecurity consulting industries. Incorporating business development, project management and threat intelligence, he works with companies around the world to identify, contain and eradicate threats from their digital environments. Brendan has worked with law firms, insurance carriers and directly with victims of complex cybersecurity compromises, maintaining active certifications as a CSI Linux certified investigator and open-source intelligence (OSINT) analyst.

A frequent speaker on the topics of digital forensics and incident response, Brendan has led discussions on the prevention and response to cyber security incidents throughout the insurance, manufacturing, healthcare, financial services, education and public entity verticals.



Terry Oehring

CEO, Solis Security



Terry Oehring, CEO, Solis Security, has over 25 years of cyber security expertise through various leadership roles in the technology and finance industries. Based in Austin, TX, Terry founded Solis in 2003 as an Information Security company focused on helping financial institutions build robust and effective security programs. With a strong focus on integrity and an exceptional commitment to their customers, Solis protects businesses from devastating cyber-attacks through Managed Security Services, Cyber Incident Response and Cyber Advisory Services.

After years of partnering with Solis to assist with their clients experiencing cyber-attacks, CFC Underwriting acquired the company. Now, by combining state-of-the-art technology and unparalleled cyber threat intelligence, Terry leads CFC Response, CFC's cyber incident response team of cyber security engineers, forensic specialists and incident responders who successfully prevent and remediate thousands of cyber events each year.

Terry Oehring attended St. Edward's University from 1997 to 1998, where they studied Computer Science. Prior to that, they were enrolled at The University of Texas at Austin from 1989 to 1991, focusing on Aerospace Engineering.

Thank You



CHARLESTON
SCHOOL OF LAW

sentinelone.com