

Privacy and Cybersecurity in the Crosshairs



Navigating Emerging Enforcement, Litigation, and Compliance Risks



NELSON
MULLINS

THE AGENDA



**INTRODUCTION:
THE PERFECT
STORM**



**EVOLVING
FEDERAL
ENFORCEMENT
LANDSCAPE**



**STATE AG AND
GLOBAL
ENFORCEMENT
TRENDS**



**PRIVATE
LITIGATION
RISKS**



**BEST
PRACTICES FOR
RISK
MITIGATION
AND
COMPLIANCE**



**NELSON
MULLINS**

I. The Perfect Storm

- Increase in private data collection
- Increase in multi-national criminal threats
- Increase in state-sponsored fraud, espionage, and attacks
- Emergence of AI tools will enable and increase threats

Increase in Private Data Collection

- Everyone is a data business - Businesses are collecting more personal data than ever before.
- Data includes sensitive information such as financial and health records.
- This increase raises privacy and security concerns, as well as regulatory risk and litigation exposure.
- Regulations are evolving to address these collection practices.



Multi-National Criminal Threats

Fraud Factories - large-scale, transnational criminal operations involving hundreds of workers

- Business Email Compromise
- Pig Butchering
- Phishing
- Romance Scams
- Tech Support Scams
- Sextortion

THE WALL STREET JOURNAL.




Posing as 'Alicia,' This Man Scammed Hundreds Online. He Was Also a Victim.

A multibillion-dollar cyberfraud industry operating out of Southeast Asia relies on forced labor and torture

ies Warn of Rising Iranian Cyber A ks, and Critical Infrastructure

 Ravie Lakshmanan

 Reuters

North Korean cyber spies created U.S. firms to dupe crypto developers

North Korean cyber spies created two businesses in the U.S., in violation of Treasury sanctions, to infect developers working in the...

Apr 24, 2025

State-Sponsored Cyberattacks

Unrestrained China

Have Stolen Data From Almost Every Amer

information collected during the yearslong Salt Typhoon attack c
allow Beijing's intelligence services to track targets from the Unite
tates and dozens of other countries.

Chinese Communi

Cyber Espionage to Un

American Economy

Impact of AI Tools on Cybersecurity Landscape

May 8, 2024

FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence

SAN FRANCISCO—The FBI San Francisco division is warning individuals and businesses to be aware of the escalating threat posed by cyber criminals utilizing artificial intelligence (AI) tools to conduct sophisticated phishing/social engineering attacks and voice/video cloning scams. The announcement, made today from the RSA cybersecurity conference at the Moscone Center in San Francisco, coincides with the division's outreach efforts to include an FBI booth at the conference and participation in multiple conference panel sessions during the week of May 6, 2024.

- AI helps us all do more, with less effort, in less time. Unfortunately, this is true for the bad guys too.
- AI excels at data collection and analysis and the automation of simple tasks - particularly important tools for professional scam artists.
- AI-driven tools increase the speed and scale of cyber threats, while making them harder to trace.

II. The Evolving Federal Enforcement Landscape

Overall trendline – it's going to be on you. Know the law, know your data, know your vendors, invest in security and compliance.

- Federal Legislative and Regulatory Developments
- DOJ's Data Security Program
- Civil Cyber Fraud Initiative

Federal Legislative and Regulatory Developments

- 1/25 - GM/OnStar banned from selling driver geolocation and behavior data
- 5/25 - Congress passed *Take it Down Act*, placed enforcement authority with FTC
- 5/25 - Attempts to preempt state-level AI regulation in BBB failed
- 6/25 - FTC Updated *Children's Online Privacy Protection Rule (COPPA)* (new parental opt-ins, limits on data retention)
- 6/25 - new FTC guidance on Safeguards Rule (non-bank fin inst must implement comprehensive security programs)

DOJ Civil Cyber Fraud Initiative

- Oct. 2021: DOJ launched CCFI to use the False Claims Act against government contractors and grantees who failed to adhere to required cybersecurity standards.
- Three targets: (1) noncompliance; (2) misrepresentations; and (3) failure to timely report breaches
- DOJ has now recovered more than \$30M (Rocketdyne, Georgia Tech) under CCFI
- Trump Administration has actively continued the policy

DOJ Data Security Program

- Run by DOJ's National Security Division, intended to protect bulk sensitive personal data from "countries of concern" (China, Cuba, Iran, North Korea, Russia, Venezuela)
- In reality, DSP imposes substantial new burdens on companies doing any kind of international business
 - Ex: If you outsource business services to an Indian vendor, and that vendor has access to the "bulk" personal data of your U.S. clients and customers, that vendor will need to comply with DSP standards. If not, your business could be on the hook for fines, penalties, and the potential for criminal prosecution.
- DSP requires that companies holding bulk personal data and doing business internationally must conduct detailed due diligence, place strict controls on their vendor contracts, and conduct regular vendor audits.
- Effective 4/2025, enforcement grace period ended 7/2025, first compliance reports come due 10/2025.

III. State AG Enforcement Trends



State Enforcement Surge

- Surge of enforcement activity in 2025, with focus on data privacy and security at the forefront (SC - UTPA)
- CCPA/CPRA out front on creating *de facto* national enforcement scheme for consumer data privacy, with other states following (CO, VA, CT, UT, OR, etc)
- With or without nationwide business, companies may find themselves pulled into state jurisdiction by web presence alone

IV. Private Litigation Risks

Bojangles class action alleges restaurant experienced weeks-long cyberattack

NASCAR announces data breach after cyberattack exposes sensitive information

Blackbaud Software Company Subject of Class Action Lawsuit Over Cyber Attack

By Jennifer L. Henn | November 26, 2020

Category: [Legal News](#)

[FOLLOW ARTICLE](#)



V. Risk Mitigation and Compliance

**Proactive
Engagement**

**Incident
Response
Readiness**

**Internal
Investigations**

Proactive Engagement Strategies

Establish

- Establish continuous monitoring of data privacy policies.

Engage

- Engage 3rd parties regularly to ensure compliance.

Conduct

- Conduct training sessions on cybersecurity best practices.

Develop

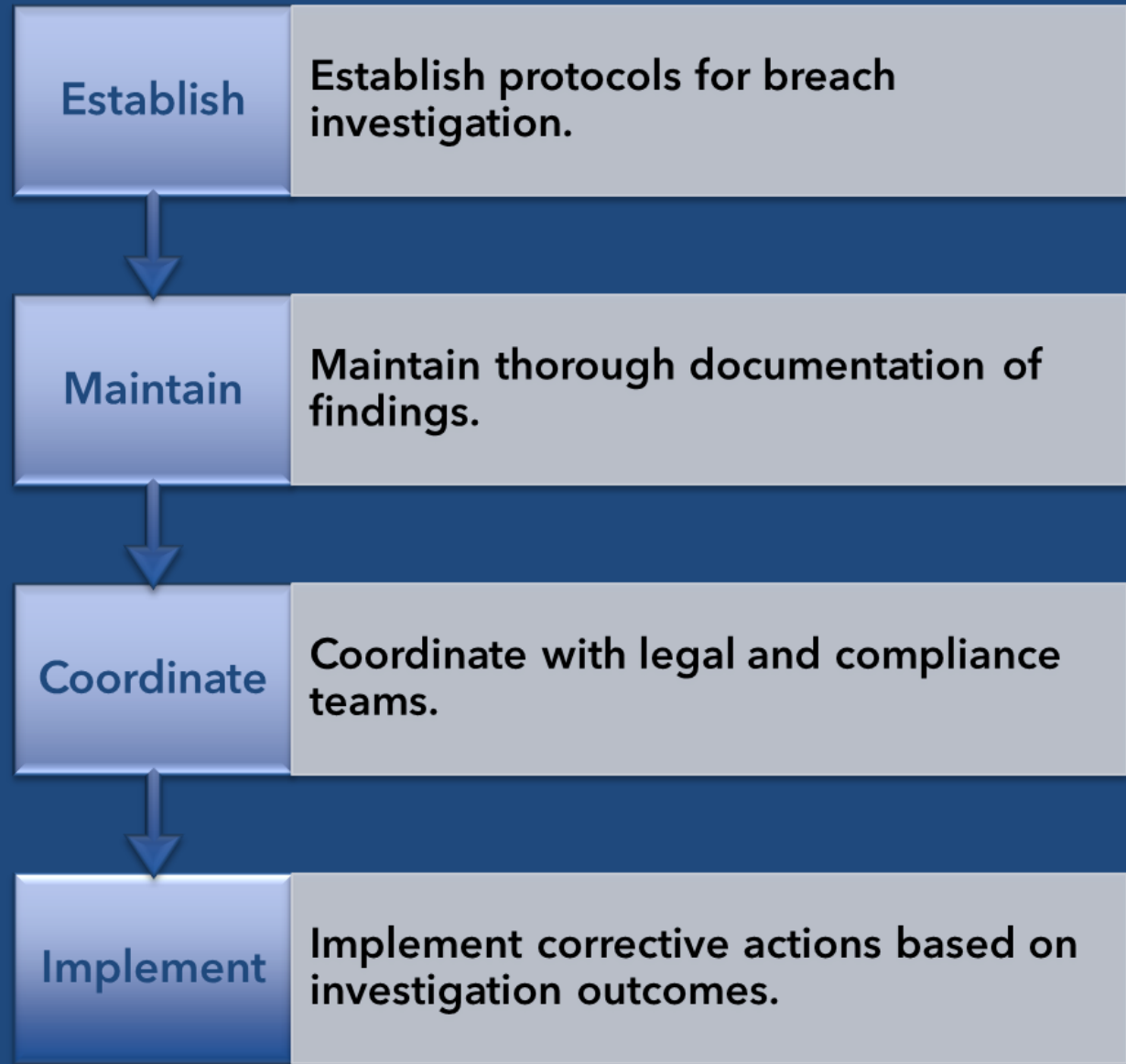
- Develop partnerships with cybersecurity firms for support.

Building Incident Response Readiness

- Establish clear roles, responsibilities, and escalation paths
- Conduct regular tabletop exercises to test and refine response plans
- Continuously update playbooks based on evolving threats and lessons learned



Executing Effective Internal Investigations



Key Takeaways

- ✓ Data security risks are rising across the globe and show no sign of slowing down
- ✓ For companies, data security failures can result in a mix of bet-the-company problems
- ✓ Companies that are proactive, prepared, and self-aware will best mitigate risk in this environment
- ✓ Know your data, know your vendors, invest in security and compliance – it's not if, but when

Thank



SHERIA CLARKE

ANNE MARIE HANSON

BROOK ANDREWS