Date

Developments in Cyber Regulation

Erez Liebermann
Debevoise & Plimpton

Josh Friedman
Meta

Drew Bagley
Crowdstrike

Privacy+ Security Forum

Overview

- Key Recent Regulations
- Cyber Regulatory Trends
- Enforcement and Litigation Trends
- Questions

Proposed NYDFS Part 500 Amendments

- **Class A Companies**: New obligations for large companies. Additional obligations include independent audits, vulnerability assessments, password controls, and monitoring.
- **Governance**: CISO independence, additional board reporting + expertise, policy approvals, CEO certification, BCDR plans, and tabletop exercises and IRPs.
- **Risk Assessment:** Tailor assessments to the specific organization with annual updates.
- **Technology**: Proscriptive requirements, including implementing policies and procedures to ensure a complete asset inventory and requirements relating to privileged accounts.
- **Notification Obligations**: NYDFS must be notified within 72 hours of unauthorized access or deployment of ransomware; within 24 hours for extortion payments + rationale.
- **Penalties**: Clarifies what constitutes a violation and provides a list of mitigating factors.

SEC Proposed Rules for Registered Investment Advisers and Registered Investment Funds

- **Risk Management**: Advisers and funds must adopt and implement policies and procedures that are "reasonably designed" to address cybersecurity risks.
- **Incident Reporting**: Mandatory reporting requirement for "significant" cybersecurity incidents.
- **Disclosure Obligations for Advisers**: Required disclosure of cybersecurity risks and incidents that could materially affect the advisory relationship with current and prospective clients.
- **Disclosure Obligations for Funds**: Requirement to report significant cybersecurity incidents and risks, similar to the required disclosures for advisers.

SEC Proposed Rules for Public Companies

- **Form 8-K Disclosure**: Mandatory disclosure of information about material cybersecurity incidents in a new Form 8-K line item within four business days of determining the incident is material.
- **Periodic Updates**: Mandatory disclosure of any material changes on Form 10-Q and Form 10K from the disclosures in the initially filed Item 1.05 8-K.
- **Risk Management and Governance**: Increases the scope and detail of registrant disclosures on cybersecurity risk management, strategy, and governance.
- **Board**: Disclosure of board expertise on cyber.

Cyber Incident Reporting for Critical Infrastructure Act of 2022

- Report "**substantial cyber incidents**" entities "reasonably believe[]" occurred to CISA within 72 hours. These are incidents that:
  - Lead to substantial losses in confidentiality, integrity, or availability of systems, or serious impacts on safety or resiliency of operational systems and processes
  - Cause business or industrial disruption; or
  - Involve unauthorized access or disruption through supply chain compromise
- Report **ransom payments** within 24 hours
- "Prompt" **ongoing reporting obligations** for "new or different information"
- **Evidence preservation** requirements
- Expanded enforcement capability, including request for information and subpoena power

Banking Agencies' Final Rule on Computer-Security Incident Notification Requirements

- Effective as of April 1, 2022
- Requires a **banking organization** to notify its primary federal regulator of any "computer-security incident" that rises to the level of a "notification incident," as soon as possible and no later than 36 hours after the organization determines that a notification incident has occurred.
- Requires **bank service providers** that experience computer-security incidents that have caused, or are reasonably likely to cause, material service disruptions or degradations for 4+ hours to notify affected banking organization customers.

Biden Administration Cyber Initiatives

- **Exec. Order 14028 on Improving the Nation's Cybersecurity** (May 12, 2021)
  - Comprehensive cybersecurity EO issued in the wake of Colonial Pipeline.
  - Directed at the federal government and its contractors to address vulnerabilities in critical infrastructure.
  - Removes barriers to sharing threat information; enhances software supply chain security and establishes a Cyber Safety Review Board.
- **Memo: What We Urge You To Do To Protect Against The Threat of Ransomware** (May 12, 2021)
  - Released concurrently with EO 14028
  - Sets out voluntary guidelines for private entities to follow to guard against ransomware.
  - Companies are urged to use the guidelines to assess readiness, but the guidelines are unlikely to impact significantly the programs of already highly regulated entities or those with otherwise mature cybersecurity programs.

TSA/DHS Cybersecurity Directive

- Focus on **critical infrastructure**, with an intention to begin formal rulemaking
- Revised July 2022 directive requires **pipeline owners and operators** to:
  - Develop network segmentation policies and controls;
  - Create access control measures;
  - Build monitoring and detection policies and procedures;
  - Test and audit for vulnerabilities and apply security patches and updates; and
  - Establish a Cybersecurity Incident Response Plan and a TSA-approved Cybersecurity Implementation Plan.
- An October 2022 directive extends these obligations to **passenger and freight railroad carriers.**

Cyber Regulatory Trends

- U.S. government taking more active approach in combatting disruptive and destructive cyber events (e.g., ransomware) and securing critical infrastructure
- Broader and earlier reporting requirements
- Patchwork of standards are beginning to unify around key data security elements
- Regulatory areas of focus:
  - Operational resiliency and cascading impacts
  - Third-party risk management
  - Data protection and minimization
  - Senior management and board engagement on cyber
  - Payments to sanctioned groups

Enforcement Actions

- **SEC Reg S-ID** (July 27, 2022): SEC findings that three separate firms failed to maintain an "adequate" program to prevent identity theft. Penalties ranged from $425,000 to $1.2 million.
- ***Aerojet* DOJ Settlement** (July 8, 2022): Aerojet agreed to pay $9 million to resolve allegations that it violated the False Claims Act (FCA) by misrepresenting compliance with cybersecurity requirements in federal government contracts.
- **SEC Reg S-P** (August 30, 2021): Eight firms settled with the SEC for failing to protect confidential customer information in violation of the Safeguards Rule. Collectively, the firms will pay $750,000 in penalties.
- **SEC *Pearson* Penalty** (August 16, 2021): SEC imposed a $1 million civil penalty on Pearson for its allegedly poor disclosure of a 2018 cyber incident, resolving charges that Pearson misled investors.
- **NYDFS Consent Order** (April 15, 2021): NYDFS imposed a $3 million penalty against National Securities Corporation for various violations of Part 500.