NYDFS Proposes Significant Changes to Its Cybersecurity Rules

August 1, 2022

On July 29, 2022, the New York Department of Financial Services ("NYDFS") released Draft Amendments to its Part 500 Cybersecurity Rules, which include a mandatory 24-hour notification for cyber ransom payments, annual independent cybersecurity audits for larger entities, increased expectations for board expertise, and tough new restrictions on privileged accounts. There will be a very short 10-day pre-proposal comments period (ending August 8, 2022), followed by the publishing of the official proposed amendments in the coming weeks, which will start a 60-day comment period.

THE SIX CATEGORIES OF DRAFT AMENDMENTS

The NYDFS's Part 500 Cybersecurity Rules first became effective in March 2017. Many other state and federal regulators in the United States quickly embraced these rules as the gold standard for cybersecurity regulation, and subsequently adopted similar requirements. International regulators have also looked to Part 500 for guidance in designing their cyber regulations. The Draft Amendments (some of which were previewed last year as part of the NYDFS's Ransomware Guidance) can be roughly divided into six categories: Obligations for Larger Companies, Governance, Risk Assessments, Technical Requirements, Notification Obligations, and Penalties.

New Obligations for Class A Companies

The Draft Amendments create a category of "Class A" companies, which are covered entities with over 2,000 employees or over $1 billion in gross annual revenues averaged over the last three years from all business operations of the company and its affiliates. Class A companies are subject to several additional cybersecurity obligations, including:

Audits. An independent audit of the company's cybersecurity program must be conducted at least annually.

Vulnerability assessments. Systematic scans or reviews of information systems must be conducted at least weekly, and any material gaps found during testing must be documented and reported to the board and senior management.

Password controls. A password vaulting solution must be implemented for privileged accounts, along with an automated method of blocking commonly used passwords.

Monitoring. An endpoint detection and response solution must be implemented to monitor anomalous activity, including lateral movement, as well as centralized logging and security event alerting.

Governance

The NYDFS views strong governance as a central aspect of good cybersecurity. The original Part 500 required cybersecurity reporting to the board, written policies approved by a Senior Officer, the need for a CISO or equivalent, among other mandates. The Draft Amendments provide several enhancements to the Part 500 governance requirements, including:

CISO independence. The Draft Amendments require that the CISO have adequate independence and authority to ensure that cyber risks are appropriately managed.

Additional board reporting. The CISO is currently required to report to the board annually on the company's cybersecurity program and material cybersecurity risks. The Draft Amendments provide for additional annual reporting to the board on plans for remediating inadequacies, as well as timely reporting to the board on material cybersecurity issues or major cybersecurity events (which are not defined).

Board expertise. Consistent with the SEC's focus on the cybersecurity expertise of board members, under the Draft Amendments, the board of covered entities will be required to have sufficient expertise and knowledge (or be advised by persons with sufficient knowledge and expertise) to exercise effective oversight of cyber risk.

Policy approvals. The board, not senior management, is required to approve the company's cybersecurity policies.

CEO certification. The annual certification of compliance must be signed by the CEO and the CISO (rather than by a Senior Officer). Under the Draft Amendments, the certification would allow for an acknowledgement of less-than-full compliance, with an identification of the specific deficiencies, but companies must be prepared to provide the NYDFS with their documentation of remedial efforts planned and underway, along with a timeline for implementation of those efforts.

BCDR plans. The Draft Amendments add significant details on the requirements for business continuity and disaster recovery plans, including designating of essential data and personnel, communication preparations, back-up facilities, and identifying necessary third parties.

Tabletop exercises and IRPs. Covered entities must periodically test (1) their incident response plans with all staff who are critical to the response, including senior officers and the CEO; (2) their business continuity and disaster recovery plans with all staff who are critical to the continuity and response effort, including senior officers; and (3) their ability to restore their systems from backups. Incident response plans must address ransomware incidents and include recovery from backups.

Risk Assessments

The Draft Amendments make several important changes to Risk Assessment requirements in Part 500, including:

Tailored assessment. The Draft Amendments expand the current definition of Risk Assessment to make clear that these assessments should be tailored to the specific organization: "Risk assessment means . . . the process of identifying cybersecurity risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, customers, consumers, other organizations, and critical infrastructure resulting from the operation of an information system. Risk assessments shall take into account the specific circumstances of the covered entity, including but not limited to its size, staffing, governance, businesses, services, products, operations, customers, counterparties, service providers, vendors, other relations and their locations, as well as the geographies and locations of its operations and business relations . . . ."

Updates. The risk assessments must be updated annually, an impact assessment must be conducted whenever a change in the business or technology causes a material change to the company's cyber risk, and Class A companies must use external experts to conduct the risk assessment at least once every three years.

Technology

The Draft Amendments also add several significant new technology requirements, including:

Asset inventory. Each covered entity, regardless of size, will be required to implement policies and procedures to ensure a complete asset inventory that tracks information (*e.g.*, owner, location, classification or sensitivity, support expiration date, and recovery

time requirements) for all hardware, operating systems, applications, infrastructure devices, APIs, and cloud services.

Access controls. The Draft Amendments expand requirements relating to privileged accounts, including requiring that (1) the access functions of privileged accounts be limited to only those necessary to perform the user's job function; (2) multifactor authentication for all privileged accounts, except for certain service accounts; and (3) all protocols that permit remote control of devices be disabled or securely configured.

Notifications

Several new notification obligations are also created by the Draft Amendments, including:

- The requirement to notify the NYDFS within 72 hours of any unauthorized access to privileged accounts or deployment of ransomware within a material part of the company's information systems.

- A new 24-hour notification obligation for any extortion payment connected to a cybersecurity event, as well as a 30-day reporting requirement explaining why payment was necessary, alternatives that were considered, and sanctions diligence that was conducted.

Penalties

Finally, the Draft Amendments clarify two aspects of the enforcement aspects of Part 500. First, they provide that the commission of a single act prohibited by Part 500, or the failure to satisfy an obligation, constitutes a violation, including the failure to comply for any 24-hour period with any section or subsection of Part 500. Second, the Draft Amendments provide a list of several mitigating factors that the NYDFS may take into account when assessing penalties (*e.g.*, cooperation, good faith, intentionality, history of prior violations, harm to customers, gravity of violation, number of violations, involvement of senior management, etc.). These mitigation factors are currently provided for in the Banking Law and therefore already apply to some regulated entities. The Draft Amendments would extend these factors to other DFS-regulated entities covered by the Insurance Law and the Financial Services Law.

NEXT STEPS

If adopted, most of the Draft Amendments would take effect 180 days from the date of adoption. The expanded notification requirements and the changes to the annual notice of certification would, however, take effect 30 days after adoption. Also, many of the

technology-related amendments (*e.g.*, new requirements for passwords, access controls and endpoint detection solutions) would take effect one year after adoption.

TAKEAWAYS

- **Comments.** Companies should closely review the Draft Amendments and consider providing comments. In the lead-up to the adoption of the original Part 500, the NYDFS was very open to industry feedback and will likely take comments very seriously in finalizing the Draft Amendments.

- **Technology.** For some companies, the proposed technology changes (especially the asset inventory requirement) may take some time to implement, and companies that will need several months to reach compliance should considering starting early.

- **Budget.** The Draft Amendments will likely take effect in 2023, and many components of the proposed new rules will require some companies to significantly increase their cybersecurity compliance budgets. In addition to the technological enhancements, new audit and risk assessment requirements may require additional resources, and covered entities should consider the likelihood of expanded budget needs for next year to adjust to these new requirements.

To subscribe to the Data Blog, please click here.

* * *

Please do not hesitate to contact us with any questions.

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com

James Pastore
jjpastore@debevoise.com

Michelle Huang
mhuang1@debevoise.com

NEW YORK

Avi Gesser
agesser@debevoise.com

Charu A. Chandrasekhar
cchandra@debevoise.com

SAN FRANCISCO

H Jacqueline Brehmer
hjbrehme@debevoise.com

Erez Liebermann
eliebermann@debevoise.com

Mengyi Xu
mxu@debevoise.com