Privacy Alert

August 2022

Significant Changes Proposed to the New York Department of Financial Services Cybersecurity Regulation

The New York Department of Financial Services (NYDFS) released proposed amendments to its Cybersecurity Regulation (23 NYCRR 500) that, if codified, will impose new requirements such as annual independent cybersecurity audits for larger entities, risk assessments for all covered entities, new technology requirements, mandatory 24-hour reporting for cyber ransom payments, new restrictions on privileged accounts, and higher expectations for board expertise to oversee businesses' cyber risk.

The pre-proposal comments period ends on Aug. 18, 2022. After the pre-proposal period, the official proposed amendment will be published, which will initiate a 60-day comment period.

In March 2017, New York became the first state to issue cybersecurity rules for banks, insurers and other NYDFS-regulated financial services companies under 23 NYCRR 500. The stringent Cybersecurity Regulation covered more than 3,000 entities, ranging from large international banks to individual insurance brokers and their third-party service providers. The impact of the regulation resulted in federal, state and international regulators implementing similar cybersecurity requirements. The NYDFS has indicated the proposed regulations are necessary to address recent cybercriminal exploitation of technological vulnerabilities to gain access to sensitive electronic data. Will federal, state and international regulators follow suit this time too?

Some of the key changes are highlighted below.

New Type of Entity: Class A Company

The proposed amendments create a new type of covered entity—referred to as a Class A company. Class A companies are covered entities with more than 2,000 employees or more than $1 billion in gross annual revenue averaged over the past three years from all business operations of the company and its affiliates.

Class A companies are subject to additional cybersecurity obligations, including:

- Audits: Undertaking an annual independent audit of the company cybersecurity program.
- Vulnerability assessments: Conducting weekly systemic vulnerability scans of information systems, and documenting and reporting to the board and senior managers any material gaps that are discovered during vulnerability assessments.
- Privileged account controls: Establishing access controls for passwords, including blocking commonly used passwords and password vaulting solutions for privileged accounts.

Attorney Advertising

- Endpoint Detection and Response (EDR) Solutions: Implementing EDR and Security Information and Event Management (SIEM) solutions to monitor information systems and provide centralized logging and SIEM alerts.

Requirements for All Covered Entities

The proposed amendments will also implement changes to all covered entities' cybersecurity policies and programs as they relate to governance, technology requirements, notification time frames and penalties.

Governance

The proposed amendments establish heightened governance requirements for all covered entities, including:

- Senior governing body. Covered entities are required to have a senior governing body (a board of directors, committee of the board or, if neither of those exists, a senior officer) that is responsible for the cybersecurity program. The senior governing body is required to have sufficient expertise and knowledge (or be advised by persons with sufficient expertise and knowledge) to exercise effective oversight of cyber risk and to approve the company's cybersecurity policies.
- Chief information security officer (CISO). The CISO has broad independence and authority to manage cyber risk. The CISO is responsible for submitting timely reports on material cybersecurity issues or major cybersecurity events and an annual report on the covered entities' cybersecurity program, including plans for remediating inadequacies and material cyber risks.
- Certification of compliance. The chief executive officer (CEO) and the CISO must sign the annual certification of compliance. If codified, the draft amendments allow for an acknowledgment of less-than-full compliance when a company identifies specific deficiencies. A company that submits an acknowledgment will have to provide supporting information that documents the identification of—and the remedial efforts planned and underway to address—the deficiencies and the timeline for the completion of the remedial efforts.
- Assessments. Covered entities must conduct a risk assessment tailored to their organization at least annually and a vulnerability assessment biannually. Additionally, covered entities must conduct impact assessments whenever a material change in business or technology impacts its cyber risk.
- Incident Response Plan (IRP) and Business Continuity and Disaster Recovery (BCDR). Covered entities must (1) periodically test their IRP with all critical staff, including senior officers and the CEO, and the IRP must address how the covered entity will handle ransomware incidents and recover from backups; (2) update and periodically test their BCDR, including key personnel and data, communications protocol, and backup strategies; and (3) periodically test their ability to restore systems from backups.

Monitoring, Asset Management and Access Controls

The proposed amendments increase the technology requirements and access controls, including:

- Monitoring and training. Covered entities must monitor and filter emails to block malicious content from reaching authorized users and to provide phishing training for users.
- Asset management. Covered entities must implement policies and procedures to ensure a complete asset inventory of all information systems and their components (e.g., all hardware, operating systems, applications, infrastructure devices, application programming interfaces and cloud services).
- Access controls. Covered entities must improve access controls for privileged accounts, including (1) limiting the number of privileged accounts and access privileges to functions that are necessary to perform the user's job; (2) periodically reviewing all user access privileges and removing accounts and access that are no longer necessary; (3) implementing multifactor authentication for all privileged accounts, with the exception of some service accounts; and (4) disabling and securely configuring all remote access protocols.

Notification Requirements

The proposed amendments have new notification requirements, including:

- Notice of cybersecurity event. Covered entities must notify the NYDFS within 72 hours of a ransomware attack on a material part of their information system or when an unauthorized user has gained access to a privileged account.
- Notice of an extortion payment. Covered entities must notify the NYDFS within 24 hours of an extortion payment, and within 30 days of the extortion payment, provide the NYDFS with an explanation of why the extortion payment was necessary and descriptions of payment alternatives that were considered and due diligence that was conducted.

Violations and Penalties

Under the proposed amendments, a violation of the Cybersecurity Regulation occurs as a result of a single prohibited act or failing to satisfy an obligation, such as the failure to notify the NYDFS of a ransomware attack within 72 hours. In assessing penalties for violating the Cybersecurity Regulation, the NYDFS will consider mitigating factors such as good-faith efforts, degree of cooperation, prior violations, harm and intentionality.

What's Next?

If adopted, the revised Cybersecurity Regulation would likely not become effective until 2023.

The majority of the amendments will become effective 180 days after the date of adoption; the expanded notification requirements and the changes to the annual notice of certification would become effective 30 days after adoption. Some technology enhancement amendments (access controls and endpoint detection requirements) will become effective one year after adoption.

To learn more about how Loeb can help you navigate the proposed amendments to the NYDFS Cybersecurity Regulation requirements, please contact a team member on our Privacy, Security and Data Innovations team.

Related Professionals

Jessica B. Lee . . . . . jblee@loeb.com
Eyvonne Mallett . . . . . emallett@loeb.com

7054 REV1 08-23-2022