Articles + Publications | December 7, 2023

New Amendments to NY DFS Cybersecurity Regulation: Big Changes for Big Companies, ?and Other Implications

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos

RELATED OFFICES

Hartford

Effective November 1, 2023, the New York Department of Financial Services issued its second amended Cybersecurity Regulation (the "Regulation," 23 NYCRR Part 500). The amendment follows extensive public comments, some of which were reflected in the Regulation. Compliance is required by April 29, 2024 (180 days after the effective date), subject to the transition dates described below. Significant changes include:

- heightened requirements for large licensees defined as "class A Companies;"
- expanded requirements for notice of cybersecurity incidents, including new requirements for ransomware and extortion payments;
- new governance requirements;
- heightened requirements for vulnerability management;
- new, specific requirements related to access privileges;
- new requirement for the review of application security;
- exclusion of government entities from definition of third party service provider;
- additional requirements for asset management and data retention;
- additional requirements for monitoring and training;
- removal of ability to use compensating controls instead of encryption;
- new requirements for incident response plans;
- adjustment to annual certification requirement, including qualification that the compliance must be "material"; and
- increase in thresholds for limited exemptions for small businesses.

There are also changes to enforcement provisions, and a new ability to request an exemption from electronic filing, as well as other adjustments to the Regulation. This article reviews the changes that are likely to be considered significant for many covered entities.

Class A Company Requirements

Under the Amendment, a “class A company” means a covered entity (i.e., a NY DFS licensee) with at least $20 million in gross annual revenue in each of the last two fiscal years from all business operations of the covered entity and the New York business operations of the covered entities affiliates, and either (i) over 2,000 employees averaged of the last two fiscal years, including affiliates, wherever located; or (ii) over $1 billion gross annual revenue in each of the last two fiscal year from all business operations of the covered entity at its affiliates wherever located. Only affiliates that share information systems, cybersecurity resources or (at least part of) a cybersecurity program with the covered entity are included.

As heightened requirements for class A companies, each class A company is required to:

- Design and conduct independent audits of its cybersecurity program based on its risk assessment.
- Monitor privileged access activity, and implement
  - a privileged access management solution; and
  - an automated method of blocking commonly used passwords for all accounts on information systems owned or controlled by the class A company and wherever feasible for all other accounts. If determined not feasible, the CISO may approve the infeasibility determination, and the use of reasonably equivalent or more security compensating controls.
- Implement (i) an endpoint detection and response solution to monitor anomalous activity, including lateral movement, and (ii) centralized logging and security event alerting, unless the CISO approves reasonably equivalent or more secure compensating controls.

The newly required “independent audit” can be conducted by internal or external auditors, who must be free to make decisions not influenced by the covered entity or its owners, managers or employees.

Notice of Cybersecurity Incidents, specifically including Ransomware and Extortion Payment

Notice had been required of certain cybersecurity events, which included “any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system.” The Regulation adds a definition of cybersecurity incident to mean a cybersecurity event that has occurred at the covered entity, its affiliates, or a third-party service provider that: (1) impacts the covered entity and requires the covered entity to notify any government body, self-regulatory agency or any other supervisory body; (2) has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity; or (3) results in the deployment of ransomware within a material part of the covered entity’s information systems. The requirement to notify the superintendent of cybersecurity incidents (previously, events) has been revised (i) to reflect the fact that elements triggering the notice requirement are now incorporated into the definition of cybersecurity incident, which now includes certain ransomware events; and (ii) to emphasize that notice is required if the cybersecurity incident “has occurred at the covered entity, its affiliates, or a third-party service provider.”

In the event of an extortion payment made in connection with a cybersecurity event, such as a ransomware attack, the covered entity must notify the superintendent within 24 hours, and within 30 days provide a written description of (i) the reasons payment was necessary, (ii) alternatives to payment, (iii) diligence performed to find alternatives, and (iv) diligence to ensure compliance (including OFAC).

New Governance Requirements

The Regulation adds a definition of Chief Information Security Officer (CISO) to mean "a qualified individual responsible for overseeing and implementing a covered entity's cybersecurity program and enforcing its cybersecurity policy."

Also relevant to the new governance requirements, the Regulation defines "senior governing body" to mean the board of directors (or appropriate committee). Absent a Board or committee, the senior governing body means the senior officer or officers responsible for the cybersecurity program.

The Regulation adds an annual approval requirement for the cybersecurity policy.

The CISO must now report on a timely basis to the senior governing body or senior officer(s) on material cybersecurity issues.

The senior governing body is required to oversee cybersecurity risk management, including by

- Having sufficient understanding of cybersecurity-related matters to exercise oversight, including the use of advisors;
- Requiring executive management to develop, implement and maintain the cybersecurity program;
- Regularly receiving and reviewing management reports about cybersecurity matters; and
- Confirming that management has allocated sufficient resources.

Vulnerability Management

The Regulation specifically requires written policies and procedures for vulnerability management, to conduct pen testing from both inside and outside the information systems, and automated scans and a manual review of systems to discover, analyze and report vulnerabilities, at a frequency determined by the risk assessment, and promptly after material systems changes. A monitoring process must promptly inform of new security vulnerabilities, which must be remediated on a timely basis.

Access Privileges and Management

The Regulation imposes specific requirements for limiting and managing access privileges, including to limit the number and access functions of privileged accounts; to review and remove unnecessary privileged accounts at least annually; to disable or securely configure protocols that permit remote control of devices; and promptly terminate access following departures.

Multi-factor Authentication

Covered entities must utilize multi-factor authentication for any individual accessing any information systems. If the covered entity qualifies for a limited exemption, then the multi-factor authentication shall be utilized for remote access to (i) the covered entity's information systems, (ii) third party application (including cloud based) from

which nonpublic information is accessible, and (iii) all privileged accounts other than service accounts that prohibit interactive login. The CISO may approve in writing the use of reasonably equivalent or more security compensating controls, which shall be reviewed at least annually.

Asset Management and Data Retention

The Regulation adds new, specific requirements for written policies and procedures related to assess inventory of information systems, including tracking, and frequency of required updates and validation.

Monitoring and Training

The Regulation adds requirements to implement risk-based controls to protect against malicious code, and training that includes social engineering.

Incident Response and Business Continuity

The Regulation expands the requirement for incident response plans to include specific and extensive provisions for operational resilience, business continuity and disaster recovery.

Annual Certificate of Compliance

The requirement for the annual certificate of compliance is revised to require data and documentation to support the certification, and which must be signed by the CISO and the highest ranking executive. In lieu of the certificate, the covered entity must file a written acknowledgment that the covered entity did not materially comply for the prior year, identify all sections of noncompliance, and the nature and extent of noncompliance; and provide a timeline for or confirmation of remediation.

Changes to Limited Exemptions

The Regulation adjusts the so-called small business exemptions, increasing the threshold for employees and independent contractors from 10 to 20, and deleting the previously confusing language related to the location or responsibility of personnel. The revenue threshold is increased from $5 million to $7.5 million, including revenues from all operations of the covered entity and New York operations of its affiliates. The threshold based on assets is increased from $10 million to $15 million.

The small business exemptions no longer apply to the requirements for multifactor authentication or cybersecurity awareness training.

The Regulation adjusts the limited exemptions as well, including to exempt certain individual insurance brokers.

Compliance and Transition Dates

As indicated above, the Regulation became effective November 1, 2023, with general compliance required within 180 days (or April 29, 2024), with certain provisions subject to transition dates:

- 30 days (December 1, 2023) for compliance with the new requirements for the annual certification of compliance, and notices of extortion payments (Section 500.17).
- One year (November 1, 2024) for compliance with the new governance requirements (Section 500.4), encryption (Section 500.15), and incident response and business continuity (Section 500.16); and for the changes to the limited exemptions (Section 500.19(a)).
- 18 months (May 1, 2025) for changes related to vulnerability scans (Section 500.5(a)(2)), access privileges (Section 500.7), and monitoring and training (Section 500.14(a)(2) and (b)).
- Two years (November 1, 2025) for the new requirements for multi-factor authentication (Section 12), asset management and data retention (Section 500.13(a)).

Therefore, the provisions related to the limited exemptions other than the small business exemptions (Section 500.19(e)-(h)); enforcement (Section 500.20); effective date ?(Section 500.21), transition dates (Section 500.22), ??and exemptions from electronic filing (Section 500.24) will be enforceable April 24, 2024.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber