wiley

NEWSLETTER

New York Cyber Regulations to Impose New and Significant Burdens on the Financial Services Industry

January 2017

The New York State Department of Financial Services (DFS or Department) continues down its path toward a new set of cybersecurity requirements for the financial services industry. In a press release issued December 28, 2016, the Department announced an updated proposed regulation intended to become effective on March 1, 2017, that "will require banks, insurance companies, and other financial services institutions regulated by DFS to establish and maintain a cybersecurity program designed to protect consumers and ensure the safety and soundness of New York State's financial services industry." There is a new 30-day comment period on this proposal (and the department made meaningful changes to this proposed regulation based on the last set of comments). While the final version may still change modestly, this proposal will impose significant new compliance obligations on the financial services industry, with a relatively short compliance timetable.

Organizations Covered

The proposal applies to a "covered entity," which means "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law, or the Financial Services Law." This covers a very broad range of companies licensed to do business in these industries in New York. The proposal also will have a significant impact on thousands of entities that are "third party service providers" to the financial services industry.

Practice Areas

Privacy, Cyber & Data Governance

This proposal will supplement other cybersecurity frameworks, including those applicable under the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLB). Unlike those laws, however, this proposal applies not only to the security of personal information, but also to "information systems" generally, as well as to "business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity." Accordingly, while companies that have implemented strong security programs under HIPAA or GLB may be in reasonably good shape under these regulations (although a new review and some additional elements certainly will be required), many companies that have not had to follow these other laws will face the need to develop a more systematic approach to overall cybersecurity policies and procedures.

Risk Assessment

As with many data security or cybersecurity requirements, a key element of this regulation involves a "risk assessment." There are specific required elements of this risk assessment (including the obligation for these steps to be ongoing). Specifically, under the current proposal, each regulated entity must conduct a "periodic" risk assessment of the entity's information systems "sufficient to inform the design of the cybersecurity program" as required by the regulation. The assessment must be "updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations." In general, the risk assessment "shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized, and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems."

In addition, the risk assessment must be formalized and documented. The formal assessment must include:

(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity;

(2) criteria for the assessment of the confidentiality, integrity, security, and availability of the Covered Entity's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks; and

(3) requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the cybersecurity program will address the risks.

Cybersecurity Program

The "Cybersecurity Program" required by the regulation is keyed to the company's risk assessment, which then triggers most of the remaining elements of the program. Specifically, each Covered Entity will need to develop and implement a cybersecurity program that will:

(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems;

(2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;

(3) detect Cybersecurity Events;

(4) respond to identified or detected Cybersecurity Events to mitigate any negative effects;

(5) recover from Cybersecurity Events and restore normal operations and services; and

(6) fulfill applicable regulatory reporting obligations.

These requirements – particularly as to documentation of these steps – will become reality in two situations – an investigation or inquiry following an actual cyberattack, or a more generalized audit or review by the department, as "All documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request."

The overall cybersecurity policy required by these provisions "shall be based on the Covered Entity's Risk Assessment" and address the following areas "to the extent applicable to the Covered Entity's operations":

(1) information security;

(2) data governance and classification;

(3) asset inventory and device management;

(4) access controls and identity management;

(5) business continuity and disaster recovery planning and resources;

(6) systems operations and availability concerns;

(7) systems and network security;

(8) systems and network monitoring;

(9) systems and application development and quality assurance;

(10) physical security and environmental controls;

(11) customer data privacy;

(12) vendor and Third Party Service Provider management;

(13) risk assessment; and

(14) incident response.

Service Provider Impacts

One of the most significant impacts from this regulation will be on the relationships between financial institutions and their service providers. The regulations impose a meaningful new contractual challenge for these providers, and will likely create real tensions, new contracting burdens, and operational challenges for vendors who will now face multiple and likely inconsistent security obligations depending on their range of financial institution customers.

Under the regulation as it now stands, each covered financial institution "shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers," again derived from the risk assessment. These policies need to address, "to the extent applicable":

(1) the identification and risk assessment of Third Party Service Providers;

(2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity;

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and

(4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

For covered entities, this means new obligations before contracts can be entered into, and during the relationship on an ongoing basis. For the service providers, there will be a need to renegotiate many contracts, along with a new and potentially very burdensome obligation to demonstrate to customers the strength of a cybersecurity program along with the need to operationalize the specific requirements of each regulated customer. It is clear – if the language remains the way it is – that this regulation will impose meaningful new requirements on these contracting relationships, many of which will be burdensome without necessarily advancing specific cybersecurity goals. Companies will need to plan for these obligations now.

Compliance Deadlines and Challenges

In general, companies are likely to have 180 days from March 1, 2017, to comply with most of the requirements. (There are certain defined requirements that have longer transition periods). Regulated companies and their service providers will need this time to prepare for and meet these significant new compliance obligations.

Some companies – those that have developed meaningful cybersecurity programs based on good business decision-making – may find that new requirements. As with many regulations and standards like this, even for these proactive companies, the new regulations may indicate some areas for new or increased focus. For the rest of the industry and their service providers – which, we can project, accounts for thousands of companies – these new requirements will create the obligation for meaningful change and increased rigor in cybersecurity programs, adding to both business risk and overall legal compliance obligations.