Securities
Regulation Daily

Wolters Kluwer

May 24, 2017

New York cybersecurity rules: What firms need to know

By Kim Peretti, J.D., LL.M and Nameir Abbas, J.D.

New York Governor Andrew Cuomo recently announced final "first-in-the-nation" cybersecurity regulations that took effect on March 1, 2017. New York's Department of Financial Services (NYDFS) will administer these rules. NYDFS first issued proposed cybersecurity rules on September 13, 2016, and issued a revised version of the rules on December 28, 2016. The final rules, issued on February 16, 2017, largely resemble the revised version of the rules issued on December 28.

While many entities potentially subject to the NYDFS rules are already required to comply with the Gramm–Leach–Bliley Act and other federal regulations and guidance in the area of information and cybersecurity, the NYDFS rules are highly prescriptive, detailed and far-reaching in scope. And while these rules are rightfully described as "first-in-the-nation," it is possible other states will follow New York's lead and implement similarly prescriptive cybersecurity rules or follow its more expansive approach to cybersecurity regulation by covering, for example, business-related information and notification for security incidents with an operational impact.

Who Is Covered, and What Is Required?

Who

The rules apply to any "covered entity," defined as "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." There is a limited exception for covered entities with, among other things, fewer than 10 employees, less than $5 million in gross annual revenue or less than $10 million in year-end total assets. According to the NYDFS website, NYDFS supervises "nearly 1,900 banking and other financial institutions with assets of more than $2.9 trillion" and "all insurance companies that do business in New York," which includes "nearly 1,700 insurance companies with assets exceeding $4.2 trillion."

What

The various mandates found in the NYDFS rules can be grouped into five categories. First, the foundational requirement of the NYDFS rules is the formulation and performance of a risk assessment. Second, based on this risk assessment, covered entities are required to craft a cybersecurity program (the "cyber program"), a cybersecurity policy (the "cyber policy") and a third-party service provider security policy (the "third-party policy"). Third, covered entities are required to maintain certain records, such as audit trails and records of compliance, for specified periods of time. Fourth,

covered entities are required to utilize qualified cybersecurity personnel and to designate a chief information security officer (CISO). And fifth, the rules require notification to the NYDFS superintendent in specified circumstances.

These regulations are particularly far-reaching because their coverage extends beyond traditional notions of personal information and customer data. Many of the various mandates found in the NYDFS rules relate to "nonpublic information," which includes certain business-related information "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."

Risk Assessment

The risk assessment is arguably the foundational requirement of the NYDFS rules. Many other requirements found in the rules expressly reference the risk assessment. For example, the cyber program, the cyber policy and the third-party policy all must be "based on the Risk Assessment of the Covered Entity."

The NYDFS rules also contain detailed procedural and substantive requirements for the risk assessment. In terms of procedural requirements, the risk assessment must be (1) carried out in accordance with written policies; (2) documented; (3) conducted periodically; (4) sufficient to inform the design of the cyber program; and (5) updated as reasonably necessary to address changes to information systems, nonpublic information and business operations.

In terms of substantive requirements, the risk assessment must allow for "revision of controls" in response to technological developments and evolving threats and must consider the particular risks facing the covered entity. The risk assessment policies and procedures must also include, at a minimum, criteria for evaluating cybersecurity risks and the integrity of information systems and nonpublic information, as well as steps for mitigating risks.

Because so many key parts of the NYDFS rules incorporate the results of the risk assessment, formulating and conducting a risk assessment is the first step to compliance.

Cyber Program, Cyber Policy and Third-Party Policy

Based on the risk assessment, covered entities must prepare a cyber program, a cyber policy, and a third-party policy.

Cyber program

The cyber program largely revolves around cybersecurity events, defined as "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." Notably, the cyber program borrows heavily from the NIST Cybersecurity framework. Covered entities are required to design the cyber program to identify cybersecurity risks, protect against unauthorized access or other malicious

acts, detect cybersecurity events, respond to cybersecurity events and recover from cybersecurity events. Covered entities also must ensure that the cyber program is designed to fulfill "applicable regulatory reporting obligations."

The NYDFS rules also contain several specific, substantive requirements for the cyber program. Among other things, the cyber program must:

- Include procedures for the secure, periodic disposal of certain types of nonpublic information that is no longer necessary for business operations or for other legitimate business purposes, except where retention is required by law or targeted disposal is not reasonably feasible.
- Implement "controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest." If encryption is not feasible, alternative controls reviewed and approved by the CISO are sufficient. However, the feasibility of encryption must be reviewed by the CISO at least annually.
- While not explicitly connected to the cyber program, the NYDFS rules also require the use of "effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access." Use of multifactor authentication is explicitly required for any individual accessing the covered entity's internal networks from an external network, unless the CISO has approved in writing the use of reasonably equivalent or more secure access controls.

Cyber policy

The cyber policy requirement revolves around the creation of various information security rules and procedures. The cyber policy must be approved by a senior officer or the covered entity's board of directors and must set forth policies and procedures for the protection of information systems and nonpublic information stored on those information systems. These policies and procedures should address, among other items, network, information and device security.

Third-party policy

The third-party policy must be designed to ensure the security of information systems and nonpublic information accessible to, or held by, third-party service providers. To the extent applicable, this includes a risk assessment of third-party service providers, as well as minimum standards, due diligence processes and procedures for periodic assessment of contracts with third-party service providers.

Documentation Requirements

There are three separate documentation requirements in the NYDFS rules. The first, overarching provision is found in Section 500.17 and requires covered entities to furnish a "written statement covering the prior calendar year" certifying compliance with the rules. The covered entity must "maintain for examination" all records, schedules and data supporting this certificate for five years. If the covered entity has identified areas needing improvement, the covered entity must document this identification as well as the associated remediation, and this documentation must also be available for inspection.

The second and more limited mandate, found in Section 500.06, applies "to the extent applicable" and requires the covered entity to "securely maintain systems" that are "designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity" for a period of five years and that "include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity" for a period of three years.

The third mandate appears in Section 500.02 and requires the covered entity to make all documentation and information relevant to the cyber program available to the superintendent upon request.

Personnel Requirements

The NYDFS rules contain two separate personnel requirements. The first, found in Section 500.04, mandates the designation of a CISO with typical responsibilities, including implementation of the cyber program and cyber policy, as well as annual reporting to the board of directors.

The second, found in Section 500.10, mandates the utilization of qualified cybersecurity personnel to manage the covered entity's cybersecurity risks and to oversee and/or perform the core cybersecurity functions of the cyber program. The covered entity is required to provide cybersecurity personnel with "cybersecurity updates and training sufficient to address relevant cybersecurity risks" and verify that key cybersecurity personnel are taking steps to "maintain current knowledge" of cybersecurity threats and defenses.

Notification Requirements

The NYDFS rules require notification to the superintendent "as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred" if either (1) notice of the cybersecurity event is required to be provided to any supervisory body; or (2) the cybersecurity event has a "reasonable likelihood of materially harming any material part of the normal operations" of the covered entity. Importantly, the NYDFS rules are among the first to require notification based on operational impact rather than data compromise.

The rules also contain a requirement that each covered entity submit, by February 15, a written statement covering the prior calendar year certifying that the covered entity is in compliance.

Effective Date and Transitional Periods

The NYDFS rules became effective on March 1, 2017, and the first certification of compliance will need to be submitted to NYDFS by February 15, 2018. However, there are a number of "transitional periods" before compliance is required. The generally applicable transitional period is 180 days. Covered entities will have one year to comply with the following requirements:

- The CISO's annual report to the board of directors.
- Monitoring and testing provisions required for inclusion in the cyber program.

- The creation and performance of a risk assessment.
- The use of effective controls for access, including multifactor authentication.
- The provision of regular cybersecurity awareness training for all personnel.

Covered entities will have 18 months to comply with the following requirements:

- Audit trail requirements for reconstruction of financial transactions and detection of and response to cybersecurity events.
- Application security requirements to be included in the cyber program.
- Limitations on data retention to be included in the cyber program.
- Monitoring of users with access to nonpublic information.
- Encryption of nonpublic information.

And lastly, covered entities will have two years to comply with requirements related to the third-party policy.

Conclusion

The NYDFS rules are truly groundbreaking. The rules are uniquely prescriptive in terms of cybersecurity measures, and compliance will require a focused and committed effort on the part of covered entities. Notably, the rules extend to business information and cyber incidents that affect business operations, rather than merely personal or customer information. These characteristics signal an expansion in regulator focus and could be an approach that others follow in future rules, regulations or guidance.