CYBERSECURITY GUIDELINES – "FIRST-IN-THE-NATION" REGULATION

WHITE PAPER
JANUARY 12, 2017

JONATHAN FOXX*

On December 28, 2016, the New York Department of Financial Services (DFS) announced that it had revised its proposed cybersecurity regulations in response to public comments that they would be too burdensome, particularly on smaller institutions. The proposed rules, which were initially announced on September 13, 2016, and set to take effect on January 1, 2017, were billed as a "first-in-the-nation regulation" to protect New York residents from cyberattacks.

The "Cybersecurity Requirements for Financial Services Companies ("Regulation") is promulgated through Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, and takes effect upon publication in the State Register.[1]

These guidelines would require banks, insurers and other financial services companies regulated by the DFS to set up a cybersecurity program aimed at protecting consumer information from cyberattacks. The revised regulation eases certain reporting and encryption requirements, and exempts small institutions from complying with certain sections of the rule.

The Regulation, as revised, is set to take effect on March 1, 2017. There is a transitional period, which is 180 days from the effective date of March 1st, with implementation timeframes layered in as exceptions granted for certain requirements, from 12 months to 18 months to 24 months. Covered entities will be required to annually prepare and submit to the DFS a Certification of Compliance[2] with the New York State Department of Financial Services Cybersecurity Regulations, commencing February 15, 2018.

In this article, I will provide a high-level overview of these guidelines. This outline is not meant to be comprehensive. However, I will hit on several salient areas of interest. Expect these requirements to

---

*President & Managing Director, Lenders Compliance Group

become a model for examination and enforcement in most other states. Lenders Compliance Group has provided risk assessments for cybersecurity, information security, and information technology based on the Federal Financial Institutions Examination Council's (FFIEC) procedures. So, my firm has experience in cybersecurity risk assessments. Given that familiarity, we now are providing an overlay for the DFS cybersecurity requirements that are promulgated in the Regulation.

Cybersecurity Program

Each covered entity – that is, any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the New York State Banking Law, the Insurance Law or the Financial Services Law – must maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the covered entity's Information Systems.

The Regulation defines a "cybersecurity event" 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. For purposes of this regulation, an information system is a "discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information," as well as any specialized system such as industrial and process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

A risk assessment must be conducted by the covered entity and the cybersecurity program must be based on that risk assessment and also be designed to perform the following core cybersecurity functions:

1. identify and assess internal and external cybersecurity risks that may threaten the security or integrity of all electronic information that is not publicly available information, known as Nonpublic Information ("NPI"), 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 NPI 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.

With respect to covered entities that have affiliates, the requirements of the Regulation permit adoption of a cybersecurity program maintained by an affiliate, provided that the affiliate's cybersecurity program covers the covered entity's information systems and NPI and meets the requirements of the Regulation. An affiliate is any Person that controls, is controlled by or is under common control with another Person.

For purposes of the Regulation, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise.

Cybersecurity Policy

Bear in mind that all documentation and information relevant to the covered entity's cybersecurity program must be made available to the DFS upon request. Preparation for the DFS's examination is necessary to meet these extensive guidelines.

Each covered entity must implement and maintain a written policy or policies, approved by a senior officer[3] or the covered entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the covered entity's policies and procedures for the protection of its information systems and NPI stored on those information systems. Just as in the case of the cybersecurity program itself, the cybersecurity policy must be based on the covered entity's risk assessment and it should 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.

Chief Information Security Officer

An important component of the Regulation is the requirement to designate a qualified individual who will be responsible for overseeing and implementing the covered entity's cybersecurity program and enforcing its cybersecurity policy. This designation is given the appellation "Chief Information Security Officer" or "CISO". The CISO may be employed by the covered entity, one of its affiliates or a third party service provider. Essentially, third party service providers (i) are not an affiliate of the covered entity, (ii) provide services to the covered entity, and (iii) maintain, process or otherwise are permitted access to NPI through the provision of services to the covered entity.

To the extent this requirement is met using a third party service provider or an affiliate, the covered entity must:

1. retain responsibility for compliance with the Regulation;
2. designate a senior member of the covered entity's personnel responsible for direction and oversight of the third party service provider; and
3. require the third party service provider to maintain a cybersecurity program that protects the covered entity in accordance with the requirements of the Regulation.

The reporting requirement in the Regulation is somewhat extensive. The CISO of each covered entity must report in writing at least annually to the covered entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report must be timely presented to a senior officer of the covered entity responsible for its cybersecurity program. The CISO is required to report on the covered entity's cybersecurity program and material cybersecurity risks.

The report by the CISO should consider to the extent applicable:

1. the confidentiality of NPI and the integrity and security of the covered entity's information systems;
2. the covered entity's cybersecurity policies and procedures;
3. material cyber risks to the covered entity;
4. overall effectiveness of the covered entity's cybersecurity program; and
5. material cybersecurity events involving the covered entity during the time period addressed by the report.

Penetration Testing and Vulnerability Assessments

There is a penetration testing requirement. For those who do not know what penetration testing is, in brief, it is a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting unauthorized penetration of databases or controls from outside or inside the covered entity's information systems.

The cybersecurity program must include monitoring and testing, developed in accordance with the risk assessment, designed to assess the effectiveness of the covered entity's cybersecurity program. The monitoring and testing must include continuous monitoring or periodic penetration testing and vulnerability assessments, and must be done periodically.

The Regulation specifically notes that "absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in information systems that may create or indicate vulnerabilities," covered entities must conduct:

1. annual penetration testing of information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and
2. bi-annual vulnerability assessments, including any systematic scans or reviews of information systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the information systems based on the risk assessment.

Risk Assessment

Lenders Compliance Group is often asked what constitutes a risk assessment for the purposes of cybersecurity. The Regulation provides clear guidance in this regards. Each covered entity is required to conduct a periodic risk assessment of its information systems "sufficient to inform the design of the cybersecurity program." The risk assessment is expected to be updated as reasonably necessary to address changes to the covered entity's information systems, NPI or business operations. Furthermore, the risk assessment must allow for "revision of controls to respond to technological developments and evolving threats" and must consider the particular risks of the covered entity's business operations related to cybersecurity, NPI collected or stored, information systems utilized and the availability and effectiveness of controls to protect NPI and information systems.

The components of the risk assessment are based on the written policies and procedures. Such policies and procedures 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 information systems and NPI, 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 those risks.

To the extent a covered entity has identified areas, systems or processes that require material improvement, updating or redesign, it must document the identification and the remedial efforts planned and underway to address such areas, systems or processes.

Third Party Service Provider Policy

I noted above that a third party service provider may be used to implement the Regulation. To expand on the requirements regarding these entities, the Regulation sets forth certain guidelines relating to them. Each covered entity must implement written policies and procedures designed to ensure the security of information systems and NPI that are accessible to, or held by, a third party service provider.

Such policies and procedures must be based on the risk assessment and should address to the extent applicable:

1. the identification and risk assessment of third party service provider(s);
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.

Moreover, such policies and procedures must include relevant guidelines for due diligence and/or contractual protections relating to third party service providers, including, to the extent applicable, guidelines addressing:

1. the third party service provider's policies and procedures for access controls including its use of multi-factor authentication[4] to limit access to sensitive systems and NPI;
2. the third party service provider's policies and procedures for use of encryption to protect NPI in transit and at rest;
3. notice to be provided to the covered entity in the event of a cybersecurity event directly impacting the covered entity's information systems or NPI being held by the third party service provider; and
4. representations and warranties addressing the third party service provider's cybersecurity policies and procedures that relate to the security of the information systems or NPI.

Cybersecurity Event

Each covered entity must notify the DFS as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event as follows has occurred:

1. Cybersecurity events of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; and
2. Cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity.

Exemptions

There are a few limited exemptions from certain parts of the Regulation, where a covered entity has:

1. fewer than 10 employees including any independent contractors, or
2. less than $5,000,000 in gross annual revenue in each of the last three fiscal years, or
3. less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all affiliates.

Obviously, in evaluating the exemption requirements, each covered entity should carefully review the Regulation to determine its applicability.

Another exemption is for an employee, agent, representative or designee of a covered entity, who is itself a covered entity. This individual does not need to develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the covered entity.

There is an exemption from many parts of the Regulation for a covered entity that does not directly or indirectly operate, maintain, utilize or control any information systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess NPI.

If a covered entity does qualify for an exemption, it must file a Notice of Exemption with the DFS.[5]

In the event that a covered entity, as of its most recent fiscal year end, ceases to qualify for an exemption, it has 180 days from such fiscal year end to comply with all applicable requirements.

Incident Response

Finally, a word about incident response. As part of its cybersecurity program, each covered entity must establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event materially affecting the confidentiality, integrity or availability of the covered entity's information systems or the continuing functionality of any aspect of its business or operations.

Such incident response plan should address the following areas:

1. the internal processes for responding to a cybersecurity event;
2. the goals of the incident response plan;
3. the definition of clear roles, responsibilities and levels of decision-making authority;
4. external and internal communications and information sharing;
5. identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
6. documentation and reporting regarding cybersecurity events and related incident response activities; and
7. the evaluation and revision as necessary of the incident response plan following a cybersecurity event.

Conclusion

In this article I have only grazed the surface of the cybersecurity requirements set forth in the Regulations. Areas additionally to be considered in structuring a comprehensive implementation would include, among other things, training and monitoring, encryption of NPI, limitations on data retention, cybersecurity personnel and intelligence, application security, and adequately maintaining an audit trail. Given the complexity of cybersecurity implementation, in building out the processes, procedures, policies, forms, and technology of cybersecurity in general, and the Regulation in particular, it is highly advisable to retain a competent compliance professional who knows the full range of applicable legal and regulatory compliance requirements as well as interfacing that individual with a fully credentialed expert in IT, information security and cybersecurity.

[1] Cybersecurity Requirements for Financial Services Companies, New York State Department of Financial Services, Proposed 23, NYCRR 500, pursuant to the authority granted by sections 102, 201, 202, 301, 302 and 408 of the Financial Services Law, promulgates Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, to take effect upon publication in the State Register.

[2] A model of the Certificate of Compliance is given in Appendix A of the Regulation.

[3] A senior officer(s) is the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a covered entity, including a branch or agency of a foreign banking organization subject to the Regulation.

[4] Multi-factor authentication means authentication through verification of at least two of the following types of authentication factors: (1) knowledge factors, such as a password; or (2) possession factors, such as a token or text message on a mobile phone; or (3) inherence factors, such as a biometric characteristic.

[5] A model of the Notice of Exemption is given in Appendix B of the Regulation.