Cullen | Dykman

New York State Proposes New Cybersecurity Regulation

September 15, 2016

The New York State Department of Financial Services ("DFS") has proposed a new regulation imposing significant new cybersecurity requirements on banks, insurance companies, and other financial services institutions regulated by DFS (the "Proposed Regulation"). The new requirements will require such institutions to, among other things, establish and maintain a cybersecurity program, create an immediate response plan for security breaches, and designate a qualified individual to serve as Chief Information Security Officer ("CISO"). The Proposed Regulation contemplates an effective date of January 1, 2017, with compliance required 180 days later.

The Proposed Regulation is subject to a 45-day notice and public comment period before its final issuance. Prior to proposing this new regulation, the DFS surveyed nearly 200 regulated financial institutions to obtain insight into the industry's efforts to prevent cybercrime.

The Proposed Regulation would require any "covered entity," defined to include any state-chartered financial institution and any foreign financial institution licensed to operate in New York, to take the measures discussed below.

Establish and maintain a cybersecurity program and a written cybersecurity policy

Each covered entity would be required to establish a cybersecurity program designed to ensure the confidentiality, integrity, and availability of the entity's Information Systems. The program must be designed to perform core cybersecurity functions, such as (i) identifying internal and external cyber risks; (ii) using defensive infrastructure and the implementation of policies and procedures to protect the entity's Information Systems, and the nonpublic information stored on those systems, from unauthorized access, use or other malicious acts; and (iii) detecting and responding to Cybersecurity Events.

Each covered entity would also be required to implement and maintain a written cybersecurity policy setting forth the entity's policies and procedures for the protection of its Information Systems and nonpublic information stored on those systems. The policy would need to be reviewed, on an annual basis, by the entity's board of directors and approved by a senior officer.

Designate a qualified individual to serve as the entity's Chief Information Security Officer

Each covered entity would be required to designate a qualified individual to serve as the entity's CISO responsible for overseeing and implementing the entity's cybersecurity program and enforcing its cybersecurity policy. This requirement may be met by using a third party service provider, so long as the covered entity: (i) retains responsibility for compliance with the Proposed Regulation; (ii) designates a senior member of its personnel responsible for oversight of the third party service provider; and (iii) requires the third party service provider to maintain a cybersecurity program that meets the requirements of the Proposed Regulation.

Each covered entity's CISO would be required to develop a report, at least bi-annually, and present it to the Board of Directors and, upon request, to the DFS. The report should include, among other things: (i) cybersecurity and Information Systems assessments; (ii) the identification of any cyber risks; (iii) proposed actions to remediate any such risks or inadequacies; and (iv) a summary of all material Cybersecurity Events that affected the entity during the time period addressed by the report.

Conduct risk assessments and penetration testing

Each covered entity would be required to conduct a risk assessment of its Information Systems. Such assessments must occur on at least an annual basis, be carried out in accordance with written policies and procedures, and be documented in writing.

Additionally, each covered entity's cybersecurity program would need to include, at a minimum: (i) Penetration Testing[3] of its Information Systems at least annually; and (ii) vulnerability assessment of its Information Systems at least quarterly.

Establish a written incident response plan

As part of its cybersecurity program, each covered entity would be required to establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event affecting the confidentiality, integrity or availability of the entity's Information Systems or the continuing functionality of any aspect of the entity's business. Such a plan must, at a minimum, address the following areas:

i. the internal processes for responding to a Cybersecurity Event;
ii. the goals of the incident response plan;
iii. the definition of clear roles, responsibilities, and levels of decision-making authority;
iv. external and internal communications and information sharing;
v. remediation of any identified weaknesses in Information Systems and associated controls;
vi. documentation and reporting regarding Cybersecurity Events and related incident response activities; and
vii. the evaluation and revision of the incident response plan following a Cybersecurity Event.

Notify DFS of any Cybersecurity Event within 72 hours of the event

The Proposed Regulation would require each covered entity to notify the DFS as promptly as possible, but in no event later than 72 hours after becoming aware of any Cybersecurity Event that has a reasonable likelihood of materially affecting the normal operation of the covered entity or that affects nonpublic information. Such events include, but are not limited to: (1) any Cybersecurity Event of which notice is provided to any government or self-regulatory agency; and (2) any Cybersecurity Event involving the actual or potential unauthorized tampering with, or access to or use of, nonpublic information. The Proposed Regulation does not specify the form of notice that must be delivered to the DFS.

The Proposed Regulation's specific timing requirement would be in addition to the existing notification obligations imposed on a New York financial institution upon discovery of a security breach. The two relevant authorities are New York State General Business Law section 899-aa, applicable to all businesses operating in the state, and the Gramm-Leach-Bliley Act ("GLBA"), applicable to all financial institutions. According to NYS GBL 899aa(8)(a), in the event that any New York residents are to be notified about a security breach, the business must also notify the state attorney general, the department of state and the division of state police as to the timing, content and distribution of the customer notices and approximate number of affected persons. Additionally, according to the 2005 GLBA Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, a financial institution should notify its regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive consumer information.

Annually submit to DFS a written statement certifying compliance with the Proposed Regulation's requirements

Finally, the Proposed Regulation would require covered entities to submit to DFS a written statement by January 15 of each year, certifying compliance with the requirements of the Proposed Regulation, in the form set forth as Exhibit A in the Proposed Regulation. Each covered entity would also be required to maintain for examination by DFS all records, schedules, and data supporting the written statement for a period of five (5) years. It is contemplated that this certification requirement would commence on January 15, 2018.

If you have any questions regarding the Proposed Regulation or cybersecurity procedures in general, please feel free to contact Joseph D. Simon at 516-357-3710 or via email at jsimon@cullenanddykman.com or Adam Barazani at 516-357-3767 or via email at abarazani@cullenanddykman.com.

Practices

- Financial Institutions and Lending
- Regulatory and Compliance

Industries

- Financial Institutions

Attorneys

- Joseph D. Simon