CARTER/LEDYARD

our resources

New York State's Revised Cybersecurity Legislation for Financial Institutions: What You Need to Know

January 19, 2017

Client Advisory
January 19, 2017 by Valentino Vasi

View the PDF.

Background

"New York, the financial capital of the world, is leading the nation in taking decisive action to protect consumers and our financial system from serious economic harm that is often perpetrated by state-sponsored organizations, global terrorist networks, and other criminal enterprises." Governor Cuomo, September 13, 2016.

With this declaration the New York State Department of Financial Services ("DFS") announced the country's first state regulation to require a cybersecurity program for financial institutions. The regulation, titled "Cybersecurity Requirements for Financial Services Companies" (the "NY Rules"), requires "Covered Entities" (banks, insurance companies, and other financial services institutions regulated by the DFS) to establish and maintain a cybersecurity program that applies to a Covered Entity's Information Systems (electronic information and electronic information processing systems).[1]

On December 28, 2016, the DFS published an updated version of the NY Rules and delayed implementation until March 1, 2017. The revisions are likely a response to criticism and concerns raised by banking and insurance industry representatives and others that the NY Rules do not distinguish between small and large financial institutions, may conflict with future federal cybersecurity rules, and are too rigid (as opposed to the best practices, risk-based approach set forth in most current guidelines[2]).

The revised NY Rules allow for more flexibility than the original version but remain a detailed, process-driven regulation. The reporting and review requirements have been lessened slightly and many of the requirements are now based on a Risk Assessment. The Risk Assessment is a review of a Covered Entity's business operations related to cybersecurity, including the Information Systems it uses and how it collects and protects nonpublic information. The Risk Assessment must be regularly revisited to consider technological developments and evolving threats.

Following is a review of the NY Rules as revised December 28, 2016.

Who Must Comply – Covered Entities

A Covered Entity is "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the [New York] banking law, the insurance law or the financial services law."

This definition covers banks, credit unions, insurance companies, mortgage lenders and mortgage brokers doing business in New York State.

There are exemptions from some of the requirements of the NY Rules for Covered Entities with: (1) fewer than 10 employees or independent contractors; (2) less than $5 million in gross annual revenue each of the past three fiscal years; or (3) less than $10 million in it and its affiliates' GAAP year-end total assets. These small entities must still maintain a cybersecurity program, have a written cybersecurity policy, conduct a periodic Risk Assessment, have a written Third Party Service Provider Security Policy and procedures for the disposal of Nonpublic Information.

If a Covered Entity does not directly or indirectly maintain Information Systems or have Nonpublic Information it is exempt from most requirements of the NY Rules. It must still perform a Risk Assessment, have a written Third Party Service Provider Security Policy and comply with data retention requirements. A Covered Entity may adopt a cybersecurity program maintained by an affiliate.

Who Is Not Covered

National banks, banks chartered in other states (and not licensed in New York State) and federal credit unions are not Covered Entities.

Who *May Be* Covered

The NY Rules were created by the DFS, which oversees banks and insurance companies. Therefore, the NY Rules do not appear to apply to New York-registered investment advisers and broker-dealers, who are overseen by the New York State Office of the Attorney General's Investor Protection Bureau. However, the DFS has not specifically excluded New York-registered investment advisers and broker-dealers from the NY Rules. The DFS likely will clarify its position regarding the applicability of the NY Rules to New York-registered investment advisers and broker-dealers sometime after the NY Rules become effective.

The Requirements

As described in more detail below, the NY Rules require Covered Entities to:

- Appoint a Chief Information Security Officer ("CISO");
- Establish a written cybersecurity policy;
- Protect information using technologies such as encryption and multifactor authentication (for example, use of a password AND a biometric characteristic);
- Conduct regular assessments, including penetration testing, vulnerability assessments, and Risk Assessments;[3]
- File an annual certification confirming compliance with the NY Rules; and
- Report to the DFS within 72 hours after a determination that a Cybersecurity Event has occurred. A Cybersecurity Event is an event "that has a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity."

Cybersecurity Program. All Covered Entities must establish and implement a cybersecurity program that includes a Risk Assessment and performs six core functions:

- Identify cyber risks;
- Implement policies and procedures to prevent unauthorized access/use or other malicious acts;
- Detect Cybersecurity Events;

- Respond to Cybersecurity Events to mitigate negative effects;
- Recover from Cybersecurity Events and restore normal operations and services; and
- Fulfill regulatory reporting obligations regarding Cybersecurity Events.

A program must also include policies and procedures for disposal of Nonpublic Information.

Written Cybersecurity Policy. Covered Entities must adopt and maintain a written cybersecurity policy that is approved by a Senior Officer[4] or board of directors (or some equivalent body or a senior officer). The policy must be based on each Covered Entity's Risk Assessment and must address all of the following areas that are applicable to the Covered Entity's operations:

- Information security;
- Data governance and classification;
- Asset inventory and device management;
- Access controls and identity management;
- Business continuity/disaster recovery;
- Systems operations and availability (requirements to protect the confidentiality, integrity and availability of Information Systems);
- Physical security and environmental controls;
- Customer data privacy;
- Vendor and third-party service provider management (must have procedures to ensure the security of Information Systems and nonpublic information accessible to, or held by, third-parties);
- Risk assessment; and
- Incident response.

Chief Information Security Officer. A Covered Entity must employ a qualified CISO who is responsible for implementing, overseeing and enforcing the cybersecurity program and policy. The CISO must submit annual reports to the board of directors (or similar governing body of the Covered Entity) detailing the integrity of the Covered Entity's Information Systems and cybersecurity program and summarizing actual and attempted security breaches. The NY Rules do not contain any clarification of experience or other requirements to help define who is a "qualified" CISO. They do state that a Covered Entity must provide cybersecurity training and verify that key personnel take steps to maintain knowledge of changing cybersecurity threats and countermeasures.

Incident Response Plan. Covered Entities must have a written Incident Response Plan designed to promptly respond to, and recover from, Cybersecurity Events. The Incident Response Plan must also identify and allocate the precise roles and responsibilities of the individuals who will carry out the actions.

Third Party Service Provider Policy. Covered Entities must have written policies and procedures covering Third Party Service Providers who have access to Information Systems and Nonpublic Information. These policies and procedures are based on the Risk Assessment and include minimum cybersecurity practices required of the vendors by the Covered Entity, regular assessments of the vendors, and that the vendors maintain their own cybersecurity policies and procedures.

Disposal of Data. Policies and procedures must provide for the periodic secure disposal of any personal Nonpublic Information that becomes unnecessary for business operations or for other legitimate business purposes, except when the information is required to be kept by law or regulation, or where disposal is not reasonable due to the method of storage of the information.

Summary of Required Reports and Records

The NY Rules require Covered Entities to make specified reports and maintain specified records:

- Annual CISO Report.[5] This report should detail, as applicable:
- how Nonpublic Information is protected and the reliability and security of Information Systems;
- the Covered Entity's cybersecurity policies and procedures;
- material cyber risks to the Covered Entity;
- overall effectiveness of the Covered Entity's cybersecurity program; and
- material Cybersecurity Events involving the Covered Entity during the period covered by the report.
- Annual Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations.A written statement must be filed by January 15 of each year with the Superintendent of Financial Services certifying that the Covered Entity is in compliance with the requirements of the NY Rule. This statement must include all "records, schedules, and data supporting this certificate."[6]
- Periodic Third-Party Vendor Assessment. Periodic assessment of third-party vendors who provide services to a Covered Entity based on the risk they present to the Covered Entity and the continued adequacy of the vendors' cybersecurity practices.

The following are requirements if a Covered Entity's cybersecurity program does not include "effective continuous monitoring," or the ability to detect, on an ongoing basis, changes in a Covered Entity's Information Systems that may create or indicate vulnerabilities:

- Evidence of Annual Penetration Test. This test should identify vulnerabilities of the entity's network security systems and demonstrate application of a "methodology in which assessors attempt to circumvent or defeat the security features of an Information System." An internal record of these tests must be maintained.
- Evidence of Twice-a-Year Vulnerability Assessment. A vulnerability test must include systematic scans or reviews of Information Systems to identify publicly known vulnerabilities and be based on the Risk Assessment. An internal record of these tests must be maintained.

Comments on NY Rules

We believe the NY Rules are based on existing best practices for financial institutions. However the amount of detail in the requirements and the frequency of some testing and reporting may tax even the most well-equipped firms.

Regardless of any flaws, because of the large number of banks, insurance companies and other financial institutions based in New York, the NY Rules will have a national impact. Therefore financial institutions should familiarize themselves with the regulations, which may provide the basis for similar rules in other states or from federal regulators.

Next Steps

If not already done:

- Ascertain whether you are covered by the NY Rules based on the type and size of your business.

If you are covered:

- Appoint a CISO and give him or her the resources to manage your Cybersecurity Program.
- Perform your Risk Assessment, including creating a list of assets subject to cybersecurity risk and assigning a risk rating to those assets.
- Perform a comprehensive review of your cybersecurity policies and governance procedures and determine whether they comply with new requirements, especially testing and reporting.
- List your third-party vendors and begin a risk assessment and diligence of each vendor. A good start is to request from each vendor a report on the status of its cybersecurity program, systems and practices.
- Review the list above of required reports and records and begin to formulate a plan (including one for use of outside vendors) and compliance schedule.
- Consider cybersecurity insurance as a way to transfer some risk.

For more information concerning the matters discussed in this publication, please contact the author **Valentino Vasi** (212-238-8877, vasi@clm.com)), any member of the Carter Ledyard Cybersecurity Practice Group (**John M. Griem, Jr.**, 212-858-8659; **Melissa J. Erwin**, 212-858-8622; or **Matthew B. James**, 212-858-8644), or your regular Carter Ledyard attorney.

Endnotes

[1] *Information System* means 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/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

[2]See the Federal Financial Institutions Examination Council's (FFIEC's) Cybersecurity Assessment Tool and guidelines (https://www.ffiec.gov/cyberassessmenttool.htm); the National Institute of Standards and Technology (NIST) framework of key, risk-based guidelines for companies (https://www.nist.gov/cyberframework); SEC (https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf) and FINRA (https://www.finra.org/file/report-cybersecurity-practices) guidelines; and the Safeguards Rule of the Gramm-Leach-Bliley Act, a federal law enacted in 1999 (GLBA), that requires financial institutions to protect the security and confidentiality of their customers' nonpublic personal information (https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act).

[3] The revised NY Rules change the requirement that the Risk Assessment be performed "at least annually" to "periodic." Annual penetration tests and (now) twice-a-year vulnerability assessments are required only if a cybersecurity program does not include effective continuous monitoring.

[4] "[S]enior 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 NY Rules]."

[5] The frequency of the CISO's cybersecurity program report was changed from twice a year to "at least annually."

[6] Data must be kept for five years.
