Getting to Grips with New York’s Cybersecurity Compliance Rules

By Shawn E. Tuma

Boards of directors must actively oversee cybersecurity, with the chairman or senior officer certifying compliance, according to a new regulation in New York that will impact companies worldwide.

The cybersecurity threat to companies is ubiquitous and no industry or region is immune. Recognizing the seriousness of this risk, the New York Department of Financial Services (NYDFS) developed proposed Cybersecurity Requirements for Financial Services Companies (the ‘cybersecurity regulations’) that became effective on 1 March 2017.

The new law, a first of its kind, contains multiple requirements for direct board involvement in cybersecurity of companies regulated by the NYDFS (covered entities) in addition to those companies that are third-party service providers for covered entities. Specifically, the board is required to take responsibility for the overall cybersecurity program, review and approve its company’s cybersecurity policy, obtain cybersecurity reports from the chief information security officer at least annually and either the board’s chairman or a senior officer must sign a written certification of compliance with the regulations on an annual basis. Those who sign off on these certifications, and their companies, must take these seriously as the NYDFS has very broad authority to investigate both civil and criminal matters that fall within its scope of authority.

Overview of the cybersecurity regulations

The NYDFS’s goal was to promote the protection of customer information and the information technology systems of businesses by establishing certain minimum standards for business to adhere to but not be overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. This is directed at protecting companies’ information systems and non-public information, both of which are specifically defined.

The cybersecurity regulations do this by focusing on three key goals that cybersecurity experts have regularly identified as being crucial to improving businesses’ cybersecurity posture. They provide an outline of essential minimum standards for businesses to implement, designate who in the organization should be appointed to lead the process and mandate top down buy-in to the process by management and the board of directors. In general, they require three key things:
1. Each company must assess its specific risk profile and design a program that addresses its risks in a robust fashion, develop policies, procedures and training for personnel to address such risks and respond to incidents.

2. Each company must designate a qualified individual to serve as its chief information security officer, responsible for overseeing and implementing its cybersecurity program, reporting on its cybersecurity program and notifying the NYDFS of any material incidents.

3. Each company’s senior management must be responsible for its cybersecurity program and file an annual certification, confirming compliance with the cybersecurity regulations or certify that it meets the criteria to be exempt.

The NYDFS designed the regulations to establish minimum standards for companies while not being overly prescriptive so that cybersecurity can remain flexible to match the relevant risks and keep pace with technological advances. These general objectives are accomplished through specific requirements designed to improve companies’ cybersecurity through a combination of technological policy-driven measures.

Though this list is not exhaustive, here are some of the specific requirements that are addressed: data governance and classification, access controls and identity management, systems and network security, penetration testing and vulnerability assessments, audit trail systems, access privileges, application security, adequate cybersecurity professionals, multi-factor authentication, data retention policies, training and monitoring of authorized users and encryption of non-public information, both in transit and at rest.

**Global impact of cybersecurity regulations**

Businesses in all industries across the US and abroad will likely be impacted by the regulations, despite being a product of New York law directed at businesses regulated by the Department of Financial Services. There are two reasons for this. First, the vast breadth of businesses that fall within the NYDFS’ authority includes financial services–related businesses in New York, including banks, insurance companies and various other financial institutions. Second, the cybersecurity regulations require that such businesses contractually obligate third parties that they do business with to comply with provisions of the cybersecurity regulations. Because so many companies do business with companies related to the New York financial services industry, the reach will be global.
“THE REACH OF THE NYDFS CYBERSECURITY REGULATIONS WILL EXPAND FAR BEYOND THE COMPANIES THAT IT DIRECTLY REGULATES TO INCLUDE, TO A CERTAIN DEGREE, THOSE COMPANIES THAT DO BUSINESS WITH THEM”

The mission of the NYDFS is “[to] reform the regulation of financial services in New York to keep pace with the rapid and dynamic evolution of these industries, to guard against financial crises and to protect consumers and markets from fraud”. It does this through its authority to take any actions necessary to:

- Foster the growth of the financial industry in New York and spur state economic development through judicious regulation and vigilant supervision
- Ensure the continued solvency, safety, soundness and prudent conduct of the providers of financial products and services
- Ensure fair, timely and equitable fulfilment of the financial obligations of such providers
- Protect users of financial products and services from financially impaired or insolvent providers of such services
- Encourage high standards of honesty, transparency, fair business practices and public responsibility
- Eliminate financial fraud, other criminal abuse and unethical conduct in the industry
- Educate and protect users of financial products and services and ensure that users are provided with timely and understandable information to make responsible decisions about financial products and services

By requiring adequate cybersecurity safeguards for companies that play a role in the financial services industry, the NYDFS is fulfilling multiple aspects of its policy objectives.

**Impact on companies that are directly regulated by the NYDFS**

The NYDFS cybersecurity regulations apply to what they define as covered entities. “Covered entity 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. Put simply, a covered entity is any entity regulated by the NYDFS.”

The NYDFS’ reach is expansive in looking only at the companies that it regulates directly. As expected, this includes banks and trust companies, credit unions, foreign bank branches, licensed lenders, health insurers, life insurance companies, property and casualty insurance
companies and savings and loan associations. There are many more companies that may not be so easily expected:

- Bail bond agents
- Budget planners
- Charitable foundations
- Cheque cashers
- Holding companies
- Investment companies
- Money transmitters
- Service contract providers (“[Any] person or entity who sells or administers a service contract and who is contractually obligated to provide service under the service contract”).

The last one – service contract providers – is extremely expansive and has the potential to pull many companies within the scope of being directly regulated by the NYDFS without those companies fully appreciating the implications.

Covered entities that meet the following criteria are exempted from some of the requirements of the regulations, although most are still required:

- Have fewer than 10 employees, including any independent contractors
- Have less than $5 million in gross revenue in each of the last three fiscal years
- Have less than $10 million in year-end assets – these entities are exempted from some, but not all, requirements of the regulations

Impact on companies that are indirectly regulated – third-party service providers to covered entities

The reach of the NYDFS’ cybersecurity regulations will expand far beyond the companies that it directly regulates to include, to a certain degree, those companies that do business with them. Section 500.11 of the Regulations specifically addresses the cybersecurity of such third parties and requires covered entities to obtain satisfactory assurances that those they do business with have adequate cybersecurity safeguards.

When thinking about one of the objectives of the cybersecurity regulations, as well as most other cybersecurity and privacy policies and frameworks, it is to protect the confidentiality, integrity and accessibility of the information and computer systems. This requires protecting the information always, wherever it may be and with whoever may have possession of it. This
also requires having protections in place for all systems that will interact with the covered entity’s network. By implementing these third-party requirements, the NYDFS is trying to ensure that a covered entity’s information is protected the same way by third parties who may receive the information is it is when it is in the custody of the covered entity. This is the same method that is used under HIPAA (Health Insurance Portability and Accountability Act of 1996) for protecting health information that is transferred from a covered entity under that framework to a business associate. Essentially, this means that third-party business partners are becoming business associates.

The cybersecurity regulations decree that a covered entity’s chief information security officer requires the third-party service provider to maintain a cybersecurity program that meets the requirements of the cybersecurity regulations. It further requires the covered entity to implement written policies and procedures designed to ensure the security of information systems and non-public information that are accessible to, or held by, third parties doing business with the covered entity. The regulations make it a requirement for their contracts via contractual provisions and/or guidelines addressing cybersecurity. They do not include an exception from some of the requirements for smaller third-party service providers, like those for smaller covered entities.

What do the cybersecurity regulations mean for all companies?

Many businesses already have relatively mature cybersecurity programs in place and for those businesses the cybersecurity regulations may not have too great of an impact. Many businesses, however, do not have such programs and are lost in the wilderness of confusion in determining what they should be doing and how they should be doing it. For those businesses, the regulations should provide a basic guide to help them develop and implement an appropriate cybersecurity program.

The regulations were released on 13 September 2016 in a non-finalized form, subject to public comment, with an initial effective date of 1 January 2017. Given the substantial feedback that was generated, they were revised significantly and re-released on 28 December 2016. Businesses should anticipate that they will be codified in substantially similar form as they are now and prepare accordingly.

The effective date was delayed to 1 March 2017, but businesses that are directly regulated by the NYDFS must begin preparing now so that they will comply with the regulations by the time the law goes into effect. Non-NYDFS regulated businesses that do business with regulated entities and have access to or hold non-public information of covered entities or their
information systems (third-party service providers) will be subject to certain mandatory requirements to ensure the covered entities’ non-public information and information systems remain adequately protected. Covered entities will be required to develop preferred contract provisions for such third-party service providers that permit the covered entity to assess their cybersecurity posture, require they implement specific cybersecurity measures to protect the non-public information and information systems, establish notification and remediation requirements in case of a cybersecurity incident, and allocate who pays the costs for such an incident.

The substantive requirements of these contracts will have little room for negotiation because they are being pushed down by the requirements of the law. Moreover, because these contractual protections are to protect the non-public information and information systems, they must flow along with such data and systems access and be pushed down to other contractors and sub-contractors who have such access.

Businesses that may find themselves in this situation need to have an adequate understanding of these requirements so that they can differentiate between those things the covered entity must do vis-à-vis those things it wishes to do when negotiating these contracts. They also need to begin preparing so that they will have appropriate cybersecurity measures in place to satisfy the requirements of the cybersecurity regulations that are passed along to them via contract and that they must then pass along to those with whom they do business where the covered entity’s sensitive personal information is being shared.

[Previously published on ethicalboardroom.com]

About the Author:
Shawn Tuma (@shawnetuma) is a cybersecurity lawyer business leaders trust to help solve problems with cutting-edge issues involving cybersecurity, data privacy, computer fraud and intellectual property law. Shawn is a frequent author and speaker on these issues and has used social media to help build his practice. He is a partner at Scheef & Stone, LLP, and a full service commercial law firm in Texas that represents businesses of all sizes throughout the United States and, through its Mackrell International network, throughout the world.