5 things FinServ firms should know about the NY cyber-law

As of March 1, 2017, banks and insurers have yet another regulation to add to their list of compliance requirements, with the enactment of New York's first-in-the-nation cyber-security regulation to protect the financial services industry (and its customers) from cyber-attacks. The regulation enforces minimum standards for cyber-security while encouraging firms to keep pace with technological advances and best practices in cyber-risk management.

The impetus behind the law, which might ultimately affect all financial services firms rather than just those based in New York, is that as the global financial services network becomes more interconnected, the risk of cyber-attack becomes more likely. Regulators are therefore proscribing stricter cyber-security requirements for FinServ firms. But for many, those requirements, and how businesses can prepare to adopt them, require some clarity.

First, let's take a look at the requirements. A review of the law reveals that financial services firms everywhere may need to rethink how they approach cyber-security risk, at both a strategy and operational level. For some firms, the law might in fact serve as a wake-up call and provide a forcing function for change. For others, it might serve as a quick diagnostic on how well they're prepared for the regulatory realities that the modern enterprise needs to address.

While businesses will need to do a thorough review with legal counsel, there are five big takeaways for compliance officers looking to be compliant with New York's new law.

1 Your firm will need to have a CISO (if it doesn't have one already).

Many but not all financial services firms have a chief information security officer (CISO), a senior-level executive—who sometimes sits in the C-suite—responsible for the overall strategy and execution of managing cyber-risk. The new law stipulates that each organization covered by the regulation is required to have a CISO. Perhaps sensing that this might be a problem for some organizations, the law further provides that the CISO can either be on staff or retained from an affiliate or third-party service provider (with additional rules). In either case, the law effectively makes the case that cyber-security in the enterprise demands executive-level leadership and accountability, which aligns with the way many top organizations are thinking.

Time will tell if individual state cyber-security requirements become the norm, but it is more than likely that the reach of New York's new regulation will extend far beyond the borders of the Empire State.

2 Your firm will need to conduct periodic risk assessments.

These assessments—of the IT systems that touch stakeholders, inside and outside the enterprise—are required to be documented and need to be carried out in accordance with written policies and procedures. This includes describing how the identified risks will be mitigated or accepted based on the assessment and how the cyber-security program will address the risks. Again, some organizations are partly set up to manage these requirements, but for others there's a lot of organizational and process work that will need to be done.

3 Your firm will also need to assess its third-party vendors.

Speaking of risk outside the enterprise, the new law provides that third-party service providers must be assessed, including a periodic view of risk and the regular provision of guidelines and/or contractual protections around security measures such as multifactor authentication, encryption, and policies and procedures.

4 Your firm will need to submit an annual filing.

In addition, the law states that each covered entity needs to submit to the superintendent a written statement regarding the prior calendar year. While this may not appear like a great burden, not all organizations are likely to be prepared for this. Imagine you're the CFO of a publicly traded company and have no resources to support audits. For organizations covered under the New York law, there will be a need for resources, process, and, again, executive-level leadership and accountability.

5 All financial service firms may soon be affected, regardless of which states they're in.

While only banks, insurers, and financial services firms conducting business in New York and regulated by the New York Department of Financial Services are in scope, the national influence of many New York financial services firms means that regulation will have an effect far beyond the city. If history is any guide, one can expect comparable state laws to follow.

For example, California S.B. 1386—which requires state residents to be notified when their unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person—became effective on July 1, 2003. Since that time, all but three states (Alabama, New Mexico, and South Dakota) have enacted similar security breach notification laws, and governments around the world have enacted—or are considering to enact—such laws.

Getting savvy through content data management

The new law's potential for national impact will force financial services firms to adopt best practices and technology to manage cyber-risk. This will likely spur change in two areas.

The first is a more strategic, business-aligned approach to managing cyber-risk that asks what the business needs to do before deciding on how to protect against threats. After all, the same digital forces that are increasing the level of threats that businesses and consumers are facing are the same forces that are providing industry leaders with new competitive advantage. The CISO—which every financial service firm will need to have—will need to align security implementation with business strategy.

Second—and more pertinent to the present discussion—the CISO will need to evaluate best practices and technology for responding to the ever-evolving and challenging regulatory landscape. In other words, to use a technology construct, CISOs need to get savvy about the regulations that inform both the strategic and tactical decisions they make.

While this might seem like a new development, a growing number of organizations have adopted a content-oriented approach to managing cyber-risk more nimbly and effectively by making use of special content libraries that harmonize the hundreds of laws and regulations that govern cyber-security—including New York's own recent addition. Such a library, whether it is developed internally, or acquired through the marketplace, can monitor federal regulatory amendments and state privacy laws, including new state sources for personal information protection, security breach, data sharing, identity theft, and notification requirements.

Time will tell if individual state cyber-security requirements become the norm, but it is more than likely that the reach of New York's new regulation will extend far beyond the borders of the Empire State. As stated at the beginning of the regulation, the financial services industry is a significant target of cyber-security threats. Adoption of the cyber-security program outlined in the regulation should be a priority for any business with information assets to protect.

The good news is that the adoption of any new law does not have to be merely a burden to IT security and compliance professionals. It can be an opportunity to rethink one's approach to cyber-security and regulation, as well as make use of content library tools that can help organizations better understand the laws with which they must comply, how to better integrate that compliance into their ongoing operations, and how those regulations might change in the future.

Mike Medsker is a director in the Integrated Risk and Management practice at Edgile, a consultancy in enterprise cyber-risk.

Section 500.02 Cybersecurity Program.

What should the NY cyber-security program require?

- Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.

- The cybersecurity program shall be based on the Covered Entity's Risk Assessment and 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 Nonpublic Information stored on the Covered Entity's Information Systems;

(2) use defensive infrastructure and the implementati on of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information 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.

- A Covered Entity may meet the requirement(s) of this Part by adopting the relevant and applicable provisions of a cybersecurity program maintained by an Affiliate, provided that such provisions satisfy the requirements of this Part, as applicable to the Covered Entity.

(d) All documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request.

Source: New York State

edgile.com

Atlanta

Austin

Seattle

Boston

Chicago

Dallas

Indianapolis

Los Angeles

Minneapolis

New York

San Francisco