CFO

cfo.com

Financial Regulators Have Cyber on Their Minds

This year, expect regulators to hold financial-services companies accountable for their cybersecurity failings.

John B. Kennedy and Michael T. McGinley, Contributors

Financial regulators, struggling to keep up with the onslaught of new threats to the public's sensitive financial and personal data, have spent the last few years examining corporate cybersecurity practices, policies, and procedures and communicating their expectations to executives.

This year, expect regulators to hold companies accountable for their cybersecurity failings. Since CFOs play a critical role in ensuring their companies are able to meet these expectations, they should stay informed about these developments.

When it comes to enforcing cybersecurity preparedness, the Securities and Exchange Commission (SEC) is Flexing its regulatory muscle more than ever before. Last year, the SEC's Office of Compliance Inspections and Examinations (OCIE) released the results of its cyber-readiness examination of 57 registered broker-dealers and 49 registered investment advisers. The examination discovered that while firms had varying degrees of cyber-preparedness, most firms reported that they had been the subject of a cyber-related incident. The report underscored the importance of the issue and confirmed what most industry executives already knew — cyber risk is a serious and growing threat.

Shortly thereafter, the SEC's Division of Investment Management released a Guidance Update to help advisers create effective cybersecurity policies. The Guidance Update noted that "cyberattacks on a wide range of financial services firms highlight the need for firms to review their cybersecurity measures," and it suggested that funds and advisers mitigate cybersecurity risk by (1) conducting periodic cybersecurity risk assessments; (2) creating strategies designed to prevent, detect, and respond to cybersecurity threats; and (3) implementing the strategy through written policies and procedures and training.

What really commanded industry attention, however, was the SEC's settlement of the first-ever cybersecurity-related enforcement action in September 2015. The message to the C-suite was clear: the SEC was now holding companies accountable for their cybersecurity missteps. Around the same time, OCIE issued a Risk Alert stating that it would be conducting a second round of investment adviser and broker-dealer cybersecurity investigations focused on assessing procedures and internal controls. OCIE has also signaled to firms that cybersecurity remains a priority by including cybersecurity examinations in its 2016 Examination Priorities.

CFTC Walks Cyber Beat

The SEC is not the only financial regulator walking the cyber beat these days—the Commodity Futures Trading Commission ("CFTC") is also pushing a cyber-focused agenda. In December 2015, the CFTC approved two important proposals amending existing regulations that will require all derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data repositories to conduct periodically five types of cybersecurity testing.

They are: vulnerability testing; penetration testing; controls testing; security incident response plan testing; and enterprise technology risk assessments. CFTC Chairman Timothy Massad strongly supported the proposed rule, stating that, given the existing threat environment, the proposal requirements "should come as no surprise." Massad also noted that "[t]he risk of cyber-attacks is perhaps the most important single issue we face in terms of nancial market stability and integrity."

The CFTC's approach is noteworthy because it represents the first attempt to regulate cybersecurity at a granular level directly via regulation, as opposed

to the cybersecurity guidance and examination guidelines issued by the SEC. Executives should be aware that the CFTC's actions could very well foreshadow a change in regulator approach to cybersecurity.

State Regulators on the March

Federal regulators are not alone in focusing on cybersecurity in the financial services industry. State regulators have their own agendas, complicating compliance efforts. Financial firms, of course, must comply with the data breach notification laws in place in most states, but financial services firms may also face additional requirements depending on where and how they conduct their business. Massachusetts, for example, requires companies with personal information about a Massachusetts resident to implement a written information security program and encrypt personal information stored on portable electronic devices.

Notably, the New York State Department of Financial Services (NYDFS) recently announced its desire to partner on cybersecurity initiatives with federal regulators, offering a concrete example of how a federal-state regulatory cybersecurity partnership may affect the financial services industry.

Late last year, the NYDFS wrote a letter to several federal regulators — including the SEC and the CFTC — unveiling potential new regulations designed to increase financial sector cybersecurity. These proposed regulations would require covered entities to maintain a comprehensive cybersecurity program meeting several requirements, including providing for documented cybersecurity policies and procedures, third-party service provider management, multi-factor authentication, the designation of a Chief Information Security Officer, and audits (e.g., annual network penetration testing and quarterly vulnerability assessments).

The NYDFS believes that there exists a "demonstrated need for robust regulatory action in the cyber security space," and suggests coordinating state and federal efforts "to develop a comprehensive cyber security framework" that addresses the most critical issues without sacrificing state autonomy. This "framework" could play an important role in changing (for better or worse) the regulatory burden firms face related to cybersecurity.

Taking Action

Federal and state regulators are so active in this space that it is easy to become overwhelmed with each new announcement about a new cyber law, regulation, or enforcement action. So how should CFOs in the financial service industry respond?

This heightened regulatory activity makes it essential for companies to set up and maintain a cybersecurity program that will pass muster. Yet a review of recent regulatory guidance reveals a surprising amount of overlap with respect to regulator expectations that should enable firms to establish and maintain cybersecurity programs that achieve both operational effectiveness and regulatory compliance. To this end, the current OCIE cybersecurity examination areas and the National Institute of Standards and Technology's Cybersecurity Framework *provide a solid basis against which firms can evaluate their own cybersecurity.*

Federal and state governments are placing enormous pressure on financial services firms to protect sensitive data and are instituting a complex and evolving array of laws, regulations, and expectations. The complex web of federal and state-level law and regulation applicable to financial services firms is likely to get more complicated in the short-term, so firms should anticipate additional regulation from regulators and keep a close watch on evolving federal-state partnerships.

Over time, the developing partnerships between states and the federal government should serve to simplify and streamline cybersecurity regulatory guidance for the industry. While CFOs should expect this to be the case, progress will be measured in years, not months.

Nevertheless, although the environment is challenging, many of the cybersecurity concepts — particularly those listed above — are applicable in both the federal and state context. The key for finance chiefs in financial executives is to commit to developing, documenting, funding, and implementing a plan based on the latest regulator guidance and commensurate to each respective firm's level of cybersecurity risk. CFO

John B. Kennedy is a partner and Michael T. McGinley an associate at Wiggin and Dana.