THE
NATIONAL LAW REVIEW

Cybersecurity Regulation in the Securities Markets

Thursday, October 12, 2017

Our latest program on behalf of the SEC Historical Society hosted a panel of current and former regulators at the federal, state, and self-regulatory organization level for a discussion of the past, present, and future of cybersecurity regulation in the securities industry.

The panel consisted of Meredith Cross, partner at WilmerHale and former Director of the US Securities and Exchange Commission's (SEC's) Division of Corporate Finance; Susan Axelrod, Executive Vice President of Regulatory Operations for the Financial Industry Regulatory Authority (FINRA); Michael Pieciak, Commissioner of the Vermont Department of Financial Regulation and President-elect of the North American Securities Administrators Association; and our colleague Timothy Burke. The panel was moderated by Professor Joel Reidenberg of Fordham University School of Law. View the video rebroadcast.

Morgan Lewis

Article By Bryan M. Connor
Timothy P. Burke
Morgan, Lewis & Bockius LLPLaw Flash

Communications, Media & Internet
Securities & SEC
All Federal

This Insight highlights the key takeaways from the discussion to help firms create and maintain critical cybersecurity policies and procedures.

Firms' Cybersecurity Policies and Procedures Face Increasing Regulatory Interest

All of the regulators on our panel reiterated what most industry actors already know—that cybersecurity is of increasing interest to regulatory bodies, especially in light of the growing number of serious cybersecurity events that have caused massive data leaks to firms and their customers.

While cybersecurity concerns are typically regulated by the SEC, FINRA, and other federal government or self-regulatory bodies, the regulators on our panel noted an increasing focus on cybersecurity regulations at the state level—with New York, Vermont, and Colorado among the first states to have specific cybersecurity regulations for financial institutions. Regulations in this sphere will continue to be promulgated in response to evolving cyber threats, and although there are varying requirements at the state and federal levels, harmonization and cooperation among state and federal regulators is crucial to ensure that firms are maintaining appropriate cyber protections.

Firms typically have viewed cybersecurity from a passive, defensive standpoint, but Commissioner Pieciak stated that firms should modify their thinking to a point where they realize that "it's not 'if' we will be the victim of a cyberattack, it's 'when.'" The regulators on the panel agreed that a paradigm shift is on the horizon that will require firms to pivot from a passive, reactive disposition to a mindset focused on proactive prevention, recovery, and response.

As cybersecurity becomes a growing concern for regulatory bodies, it is expected that companies will be required to respond to these demands at the director and executive levels. Tim Burke referenced SEC Chairman Jay Clayton's public statements calling for public companies to have a board seat designated as each company's point person on cybersecurity.

Focus on Cybersecurity Insurance

Both Ms. Axelrod and Commissioner Pieciak highlighted the growing cybersecurity insurance market and lauded those companies that are leading the charge in obtaining cybersecurity insurance policies. Cybersecurity insurance is designed to mitigate losses from the many types of "cybersecurity events" that firms deal with on an

ever-increasing basis. Regulators are interested in the cybersecurity insurance market because it encourages firms to create robust cybersecurity protocols in exchange for greater levels of insurance coverage. While firms may at first shy away from the up-front costs of these policies, the costs may pale in comparison to the financial and reputational losses a firm could suffer in the wake of a serious cyberattack.

Heed the Regulators' Guidance

Former Director Cross and Ms. Axelrod stressed the importance of heeding the guidance provided by the substantive policies promulgated by the SEC and FINRA as well as looking to enforcement actions involving cybersecurity breaches to inform best practices. Some examples of such guidance can be found in the SEC's August Risk Alert, which highlights the successes and failures of 75 firms as outlined by the Office of Compliance Inspections and Examinations.

While the firms covered in the Risk Alert displayed an obvious improvement from the outlook of prior years (in that nearly every firm had comprehensive cybersecurity policies and procedures), many firms had protocols that were either lightly enforced or largely unenforced, and some had security measures or procedures that were out of step with the type of information the companies keep and the type of businesses they operate.

The regulators on our panel cited the need for greater specifics in policies and stressed that firms must keep policies and procedures that are reasonably designed to provide strong security that is tailored to a firm's particular business but also flexible enough to respond to evolving threats. All of our panelists agreed that the regulatory bodies' primary focus in the cybersecurity sphere thus far has been on informing firms of issues of concern. That said, Ms. Axelrod emphasized that—due to the vast amount of public knowledge about cybersecurity issues—firms cannot feign ignorance about the threats they pose. This makes it imperative that firms demonstrate diligence in keeping up with the latest developments in cybersecurity regulation in order to avoid enforcement actions that can lead to hefty fines and public reprimand.

FINRA, the SEC, and many other regulatory bodies regularly publish cybersecurity updates and guidance documents, and firms should exercise vigilance in keeping abreast of the most recent trends in cybersecurity enforcement and regulation—at all levels.

"The Enemy Within"

When firms consider their cybersecurity protocols, the obvious focus is on keeping internal information safe from external threats. While this is sound thinking, Ms. Axelrod, Commissioner Pieciak, and former Director Cross all emphasized that firms need to take appropriate steps to mitigate the risks of both external *and* internal threats. Of importance to our regulator panelists was a recent case in which an employee of a major financial institution was able to download—due to a programming flaw that granted him far more access to sensitive information than was necessary for his business purposes—the account information of hundreds of thousands of the firm's clients to a personal server. This employee's server subsequently fell victim to a third-party hack, which resulted in the firm's customer information being posted for sale online for a brief time. The firm quickly responded to the breach, determined who was responsible, and made the appropriate disclosures to regulators and clients. Even given the firm's appropriate remedial measures, it was fined $1 million for allowing such a wide-ranging internal cybersecurity breakdown to occur.

This case is just one example of the importance of a firm's duty to disclose cybersecurity events in the immediate aftermath of their occurrence. Such disclosures encourage transparency and allow regulators and/or law enforcement authorities to take appropriate steps to ferret out the malevolent actors. A lack of disclosure, however, not only leaves firms less ready to respond to the next cybersecurity event but—as recent events have shown—also leaves firms vulnerable to extensive reputational risk and the loss of public good will.

Third-Party Liability

Ms. Axelrod specifically pointed to the necessity of firms taking responsibility for the risks that come from utilizing third-party vendors for data storage, payment processing, and a myriad of other services. While noting that "perfection is not the standard," she stated that it is imperative that each firm have robust cybersecurity policies and procedures and "adequate and reasonable oversight to ensure that [vendors are] compliant with company policies."

Indeed, regulatory bodies at all levels are placing more emphasis on firms ensuring that their vendors are compliant with established policies and procedures, and when cybersecurity events occur, holding firms at least partially responsible for the losses and outages attributable to the firm's third-party vendors. Firms must take care to select vendors diligently and to enter into contracts that contemplate the attribution of risk should a cybersecurity event take place.