Cybersecurity Risk Management for the Securities Industry

By Emily Westridge Black and Christopher Quinlan

Emily Westridge Black is an attorney in the Austin office of Haynes and Boone, LLP. **Christopher Quinlan** is an attorney in the Dallas office of Haynes and Boone, LLP. Ms. Black and Mr. Quinlan focus their practice on data security investigations and litigation, white collar defense, and complex commercial litigation. They regularly speak and write on cybersecurity and privacy issues.

Introduction

Increasing regulatory scrutiny of cybersecurity measures is unsurprising in light of the growing prevalence and awareness of cyber threats in the United States. From Target to Sony, recent high-profile data breaches have illustrated the potentially severe consequences of a cyber-event and the diversity in the types of attackers (*e.g.*, hacktivists, advanced persistent threats, and criminal rings), motivations (*e.g.*, political activism, theft of trade secrets and other information that can be monetized), and techniques (*e.g.*, spear-phishing, zero day exploits, and malware) that give rise to cyber-attacks. From the broadly targeted SQL injection attacks, which target companies that have insecure websites and/or web applications, to sophisticated, targeted attacks on companies that may have financially or politically sensitive information, there are a large range of potential cybersecurity threats. However, the focus on these massive attacks on prominent companies may obscure one critical point: every company has valuable data and every company is a potential target for cyber-attacks.

The omnipresent risk that companies face is likely part of what motivated President Obama to identify cybersecurity as a leading threat to national security. As business and digital technology become increasingly integrated, cybercrime, political crime and financial crime merge. Nearly every transaction of substance in the modern economy is conducted in whole or in part online, and registered broker-dealers and investment advisors are in a unique position of vulnerability. Not only do they maintain financial information valuable to opportunistic criminals, but they play a critical role in national and global markets that, if undermined, could result in severe consequences. As a result, an effective approach to cybersecurity concerns is particularly important for companies in the securities industry. This article provides an overview of the regulatory backdrop for cybersecurity in the securities industry, and then provides information about how such companies can carefully assess their cyber-risk profile, their appetite for risk,

©2015, Haynes and Boone LLP

their security measures, and their mechanisms (if any) for transferring the costs of potential cyber events.

Recent Initiatives by Regulators Reflect Growing Concerns over Cybersecurity

The Securities and Exchange Commission ("SEC") and the Financial Industry Regulatory Authority ("FINRA") have shown increasing interest in assessing cyber-preparedness and setting cybersecurity standards in the securities industry. Beginning in January 2014, FINRA conducted a sweeping assessment of firms' approaches to managing cybersecurity threats. FINRA identified four broad goals of the assessment: (1) to better understand the types of threats firms face; (2) to increase FINRA's understanding of firms' risk appetite, exposure and major areas of vulnerabilities; (3) to better understand firms' approaches to managing cybersecurity threats; and (4) to share observations with industry participants.

Then in March 2014, the SEC sponsored a Cybersecurity Roundtable and emphasized the importance of cybersecurity at registered entities to the integrity of the market system and the need for effective cooperation between government and the private sector to respond to increasing cyber threats. Shortly thereafter, in April 2014, the SEC Office of Compliance Inspections and Examinations ("OCIE") announced that it would conduct a cybersecurity examination of more than fifty registered broker-dealers and investment advisors.[1] This examination included information requests inquiring about "cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain cybersecurity threats" as well as maintenance of insurance covering cybersecurity incidents.

Other regulators are also focusing on cybersecurity. For example, in December 2014, the New York State Department of Financial Services ("New York DFS") released a letter announcing the expansion of its examination procedures to focus more on cybersecurity issues at the entities it regulates.[2] The New York DFS subsequently sent letters to industry participants requesting descriptions of their cybersecurity measures. In addition, the Federal Trade Commission ("FTC") has expanded its efforts over the past year to bring cybersecurity and privacy enforcement actions under Section 5 of the FTC Act, which prohibits deceptive and unfair practices.

The OCIE and FINRA Reports Reveal Common Industry Practices and Provide Insight into Regulators' Expectations for Cybersecurity

On February 3, 2015, OCIE issued a risk alert reporting the findings of its industry examination, and FINRA issued a report identifying effective practices for dealing with cybersecurity threats.[3] OCIE and FINRA made several significant findings in their February 3, 2015 publications. OCIE's review of cybersecurity policies revealed that the majority of firms:

- Maintained written information security policies;
- Conducted periodic, firm-wide cybersecurity risk assessments;
- Conducted firm-wide inventories of technology resources;
- Made use of encryption of some type; and
- Provided their clients with suggestions for protecting sensitive information.

Many firms that were examined reported membership in an industry group or organization that existed for the purpose of sharing information related to cybersecurity (for example, the Financial Services Information Sharing and Analysis Center, or "FS-ISAC").[4] Membership in these groups is beneficial because it keeps members abreast of key cyber threats and provides a forum for discussing and developing best practices for cybersecurity. Membership is also affordable. For example, small companies may receive limited critical notifications from FS-ISAC for free or basic membership for $250.00 per year (details are available at https://www.fsisac.com/join).

The OCIE report showed that, generally speaking, broker-dealers have a more robust approach to cybersecurity than investment advisers. For example, many broker-dealers have created a dedicated Chief Information Security Officer ("CISO") position, but less than a third of advisers have done so; instead, advisers usually assign information security responsibilities to the Chief Technology Officer ("CTO"). CTOs are typically responsible for ensuring that an organization's technology portfolio is cost-effective, efficient, and always available. These objectives differ from – and can

conflict with – data security objectives, which include legal and regulatory compliance and risk mitigation. Separating responsibility for technology and security can help ensure that each objective is given appropriate consideration by avoiding creating conflicts of interest within a role. Also, most broker-dealers incorporate cybersecurity requirements into contracts with vendors and business partners, while few advisers do the same. This can be problematic because attackers can exploit vendors' vulnerabilities to attack companies. For example, attackers were able to gain access to Target's network through credentials they stole from a vendor that monitored the HVAC systems at Target stores. Finally, over half of the examined broker-dealers maintain insurance for cybersecurity incidents, while only a small number of advisers do so.

As business and digital technology become increasingly integrated, cybercrime, political crime and financial crime merge. Nearly every transaction of substance in the modern economy is conducted in whole or in part online and registered broker-dealers and investment advisors are in a unique position of vulnerability.

The FINRA report identified several effective practices for dealing with cybersecurity threats including:

- Establish a sound governance framework;
- Utilize risk assessments and technical controls;
- Develop cyber-incident response plans;
- Manage cybersecurity threats related to vendors and partners;
- Train staff on cybersecurity issues; and
- Participate in intelligence-sharing opportunities.

FINRA stated that it "expects firms to consider the principles and the effective practices presented in this report as they develop or enhance their cybersecurity programs."

Cybersecurity is an Important Component of a Company's Long-Term Business Plan

Increased regulatory scrutiny from the SEC and FINRA is not the only incentive for investment companies to develop a comprehensive plan for dealing with cybersecurity concerns. Clients and contractual counterparties are increasingly aware of the risks associated with cyber-events. Companies that suffer a substantial breach can face hundreds of thousands or millions of dollars in investigation and remediation costs, as well as massive intangible losses, including loss of intellectual property, interruption of operations, and loss of goodwill. In some instances, poor cybersecurity and/or ineffective management of a cyber incident can result in enforcement actions, litigation from investors, counterparties, and others, and the resignation of key executives. As cyber-attacks become increasingly prevalent, companies should invest in incorporating strong cybersecurity into their long-term business plans.

Minimizing Exposure to Cybersecurity Risk

Developing an effective approach to cybersecurity is a firm-specific endeavor. There is no one-size-fits-all solution. Even similar firms in the same industry may have drastically divergent technological and organizational structures that may affect their cyber risk profile. Nonetheless, the following common features of effective cybersecurity plans are generally applicable to investment companies notwithstanding the idiosyncrasies of individual firms.

Choose a Strong Cybersecurity Team

A critical first step in developing an effective approach to data security is to choose the right information security team. Data security concerns implicate a number of different departments, and cyber-events have wide implications that can affect a business in a number of ways. As a result, an effective security team should be cross-sectional, and include personnel from legal, information technology, human resources, and communications or public relations departments. The team should also include at least one member of senior management. Once the team is assembled, ensure that they have sufficient resources and authority to address the cyber risks the company faces. A penny of prevention may well be worth a pound of cure in the event of a cyber-attack.

Understand the Legal and Regulatory Landscape

In order to craft an effective approach to privacy and data security, companies should conduct a "privacy survey," which is the process of identifying the legal and regulatory landscape that applies to companies in the industry and to the types of data that the company collects and maintains.

Increased regulatory scrutiny from the SEC and FINRA is not the only incentive for investment companies to develop a comprehensive plan for dealing with cybersecurity concerns. Clients and contractual counterparties are increasingly aware of the risks associated with cyber-events.

Depending on the size of the company and the types of data collected, the scope of this survey may range from simply analyzing applicable federal and state laws and regulations and company policies, to a more detailed and complex analysis of international data protection regimes, industry standards, audit protocols, and internal policies related to vendor contracting.

SEC and FINRA scrutiny of industry cybersecurity measures is based on two SEC regulations: Regulation S-P and Regulation S-ID. Under Regulation S-P, broker-dealers and investment advisers must establish reasonably-designed, written policies and procedures to ensure the security and confidentiality of customer records and information. Investment companies must protect against any anticipated threats or hazards to the security or integrity of customer information and must protect against unauthorized access to customer records that could result in substantial harm or inconvenience to customers.

Similarly, Regulation S-ID focuses on preventing identity theft. Under Regulation S-ID, companies are required to create and maintain reasonably-designed policies and procedures designed to promote identification, detection, and response to red flags for identity theft. Regulation S-ID compliance policies must be updated periodically and be approved by senior management. The company must train its staff to implement the identity theft program and exercise appropriate oversight of third-party vendors. Annual reports must be provided to the board of directors or senior management.

In addition to these SEC regulations, also consider applicable federal and state laws. For example, the Gramm-Leach-Bliley Act ("GLBA") requires organizations to protect banking and financial information and has direct application to the securities industry. The GLBA requires the establishment of appropriate standards that insure the security of customer records and protect against anticipated threats and unauthorized access to such information that could result in harm or inconvenience to the customer. Additionally, many states have laws that require companies to protect "personally identifiable information" ("PII") of customers and employees and to notify individuals if their PII is breached. Although the definition of PII varies from state to state, PII generally covers data that can be used to identify a specific individual including social security numbers, driver's license numbers, financial account information, and other identifying information.

When conducting a privacy survey, organizations must also consider any contractual obligations that relate to cybersecurity. When the company will be responsible for maintaining a third party's data, the company should consider whether the contract creates additional cybersecurity obligations or cybersecurity liability in the event of a breach. When the company's data will be maintained by a third party, the company should take care to enter contracts that ensure that the company's data will be protected. This is important both to limit the company's exposure to cybersecurity liability as well as to protect its interests in preserving the confidentiality of any trade secrets or other proprietary data.

Finally, a privacy survey should include any of the company's applicable policies, including: data retention and destruction policies, privacy policies, data security procedures, data breach notification plans, new hire and other employee training material, computer-use agreements, and internal auditing and monitoring processes.

If You Don't Need It, Don't Keep It

Cyber criminals cannot steal what you do not have. SEC regulations require investment companies to collect and maintain extensive records, many of which may contain sensitive information (including PII) that could expose the company to liability in the event of a breach. Other data must be maintained

for practical business purposes. However, from a liability perspective, companies should collect as little sensitive data as possible within their regulatory and practical constraints, and they should only maintain that data for as long as required for business or regulatory purposes. The less sensitive data that a company has, the less desirable it is as a target for cyber-attacks and the less liability it faces if breached. The information security team should be aware of what types of data the company is required to collect and maintain. It should create, enforce, and regularly update specific policies limiting the data collected and maintained by the company and providing for the destruction of data that is no longer needed and that the company is no longer required to keep.

Understand Data and Technical Systems

Once the information security team has completed the privacy survey and taken steps to minimize the company's data collection and retention, it should identify where sensitive data is stored. (This will include data protected by law, data protected by contract, personally identifiable information, and proprietary data.) The company should have a specific and detailed understanding of its own network.

Next, the team should ensure that sensitive data is segregated from regular data and subject to additional physical, technical, and/or procedural protections. For example, the company might:

- Segment its network to separate sensitive data from non-sensitive or public data, and use technical protections, such as firewalls, to protect the sensitive segments.
- Use password protection and, where practicable, encryption to increase the security of sensitive information.
- Identify and monitor each point of access to the portions of its network that house sensitive data.
- Restrict physical access to hardware (including servers and computers) and physical files containing sensitive information.

Implement "Privacy by Design"

The company should take a "privacy by design" approach when developing cybersecurity solutions. This means that the company should create policies and procedures that account for customer privacy, legal compliance, and data protection throughout the data lifecycle (*i.e.*, collection, processing, storage, and destruction). As part of this effort, the company should develop comprehensive policies to address privacy and data security, including:

- A "bring your own device" (BYOD) policy governing whether, and under what circumstances, employees can use their own devices to conduct company business. Given the record-keeping requirements for securities firms, the BYOD policy should also address when and how information is backed up to the company's servers. If employees are permitted to use their own devices, they should be required to use password protection, install company approved security software, and to have remote wiping capabilities. (Note that remote wiping may conflict with record-keeping requirements if business-related materials are not backed up.);
- A password policy requiring the use of strong, complex, unique passwords that they change regularly and cannot be shared;
- A network tracking policy requiring regular monitoring of network traffic for evidence of suspicious access; and
- A testing policy designed to test compliance with other policies and procedures.

It is important to establish a well-developed data security plan that includes multiple layers of protection to prevent unauthorized access to sensitive data.

Train Employees

Regardless of the industry, employees are a frequent source of data breaches. To combat this, the company should clearly establish that it takes data security and unauthorized computer access seriously. Many cyber-attack techniques exploit employees' inattention and lack of technical expertise. Even a single inattentive or untrained employee can expose the company to a major breach. Employees need regular training on how to identify and prevent attempted cyber-attacks. For example, to reduce susceptibility to spear-phishing attacks, employees should be trained to carefully examine emails for indicia of fraud (*e.g.*, an email domain name that is incorrectly spelled) and instructed to never click on links sent to them via email. Similarly, to reduce the likelihood of malware attacks, employees should be instructed not to download unknown files or programs or to use unfamiliar external storage devices (*e.g.*, thumb or flash drives). Perhaps most importantly, employees should be trained to recognize when they have fallen victim to cyber-attacks and should know

the proper procedures for reporting the problem. Too often, compromised employees are reluctant to report that their conduct may have exposed the company, and their silence allows a reparable problem to grow into a critical issue. The company should cultivate an atmosphere of open communication regarding cyber-events.

Mitigation of cyber-attacks is as important as prevention.

Employees may also cause a breach or cyber-attack intentionally. This is particularly likely when employees leave an organization, especially if they leave to work for a competitor. The company should protect itself from the liability associated with unauthorized use of competitor data by incoming employees and from the risk of appropriation of the company's data by outgoing employees. The company should require certifications from new employees that they are not bringing competitor information and should instruct employees to report impermissible use of competitor information. Similarly, the company should enact policies that place clear and appropriate limitations on employee use of company resources and data. The company should terminate departing employees' access to information systems (including email) and company premises immediately after terminating their employment. Departing employees should be expressly asked whether they are taking any company information with them, and their answers should be documented in writing during the exit interviews. Employers should immediately demand the return of impermissibly taken information.

Help Investors Help Themselves

Securities firms should ensure that their investors and partners understand how to protect themselves and their investments online. OCIE released an investor bulletin that provided tips on how to better protect online investment accounts. These tips include:

- Require investors to choose a strong password (and regularly change it);
- Use two-step verification for account access; and
- Remind investors that they should exercise caution on public networks.

Companies may choose to send regular security reminders to their investors to encourage safe practices.

Prepare in Advance for the Possibility of a Cyber-Attack by Developing an Incident Response Plan

Unfortunately, even with the strongest cybersecurity measures, a company will never be "breach-proof." Even sophisticated and comprehensive cybersecurity measures can be circumvented by rogue employees or defeated by determined attackers. Cyber criminals employ a wide variety of methods to attack companies and access protected data and those methods are constantly evolving. Therefore, mitigation of cyber-attacks is as important as prevention. Effective information security promotes early detection of intrusions and the ability to quickly and effectively boot attackers from the network. Companies should coordinate with information technology professionals to monitor access to sensitive information and be on the lookout for suspicious activity. To facilitate this, companies should ensure that firewall logs are regularly reviewed and are sufficiently verbose to indicate when an intrusion (or any exfiltration of data) occurs.

A key component of any company's data security plan is the incident response plan, which is a detailed plan that governs how a company should respond to a suspected cyber-event. These plans help companies quickly and effectively investigate and remediate attacks. Among other things, an incident response plan should identify the leaders of the response team and present easy-to-follow, scenario-based responses to different types of cyber incidents. For each scenario, the plan should clearly delineate the first steps that must be taken and include a timeline of major investigative events. The plan should also provide guidance on the timing and substance of appropriate disclosures.

The plan should also provide for the involvement of professionals, as appropriate. For example, companies should involve legal counsel in all aspects of the investigation of a suspected cyber-event (including communications about the potential event, remediation efforts, and disclosure and reporting) to ensure that the investigation is protected under the attorney-client and work product privileges. Privilege is critical because, although the company is a victim, it may soon find itself the defendant in a variety of lawsuits, including lawsuits by regulators or investors. Accordingly, incident response plans should identify an experienced data security attorney to call and include their emergency contact information. For some types of adverse events, it may also be necessary to hire a forensic investigator to preserve, collect,

and analyze the relevant evidence. Typically, forensic investigators should be retained by an attorney so that their work will also be protected by privilege; however, response plans may identify potential forensic firms to contact in the event of a cyber-incident.

Prompt identification and response to a cyber-event are critical. The longer a cyber-event lasts, the more damage it can cause to the company (*e.g.*, in terms of volume of stolen data, lost access to its network, lost employee time, and potential liability to third parties). By preparing a comprehensive incident response plan in advance, the company can ensure that it takes action in a timely manner without risking costly missteps or oversights.

Execute the Incident Response Plan Efficiently

Once a company becomes aware of a suspected cyber-attack, time is of the essence. Losses from the attack are likely mounting, the clock is running on the organization's legal rights and obligations, and potential liability to claims by regulators and plaintiffs begins to mount. Even the most extensive incident response plan is of limited value if the company does not execute it efficiently.

It is important to contact the legal counsel identified in the incident response plan immediately. Experienced legal counsel will help execute the incident response plan while maintaining privilege, and can help determine where departure from the pre-established plan is necessary.

The attorney should counsel the company to avoid drawing premature conclusions regarding the cause and source of an attack and whether the attack has resulted in unauthorized access or exfiltration of data. It often takes days or weeks to determine the nature and extent of an attack. Companies should avoid making damaging, unconfirmed, and potentially inaccurate statements during cyber investigations. Companies should also avoid using the term "breach" unless it confirms that a breach has actually occurred. A "breach" occurs when information is accessed or taken by unauthorized parties. Breaches often trigger legal or contractual obligations, including disclosure of the breach. However, many cyber-attacks (*e.g.*, denial of service attacks) do not result in a breach. Imprecise, inaccurate, or reckless communications during an investigation can hinder an organization's ability to defend against charges of liability by affected third parties or regulators. In our experience, it is particularly critical to counsel employees involved in the incident response to be cautious about how and what they communicate.

After the initial investigation is sufficiently complete, legal counsel can help companies decide whether and how to contact law enforcement agencies (if they have not already become aware of the incident). Law enforcement has access to investigative tools (for example, grand jury subpoenas and search warrants) that are not otherwise available to private sector entities and are currently very interested in investigating cyber incidents that affect national security or have significant economic implications. However, law enforcement cannot and will not assist companies in repairing damage to their computer network like independent forensic investigators can, and businesses may lose control over an investigation once law enforcement becomes involved.

Legal counsel (and, often, public relations experts) will assist with any disclosures to investors, other contractual-counterparties, or regulatory agencies that may be required as a result of a material breach. Legal counsel will work to limit any harm to the company (including any reputational damage) while at the same time limiting legal liability by avoiding sweeping or inaccurate statements. Consider coordinating all communications with third parties through a single source to ensure that communications are authorized, accurate, consistent, and timely. A customer hotline or website can be useful in this regard.

Counsel should also help companies prepare for and navigate the various types of litigation and regulatory actions that may result from a cyber-incident.

Develop a Business Continuity Plan

Cyber-attacks may also result in victim-companies losing access to their data and systems. For example, many companies have been affected by the Cryptolocker malware, which encrypts (and renders useless) the company's data unless and until a ransom is paid. If companies are not prepared for these types of attacks, they may suffer a substantial interruption of services that can be extremely costly. The company should have a written business continuity plan to facilitate rapid and efficient data recovery and resumption of operations. The first step in creating an effective business continuity plan is identifying critical systems. Systems should be prioritized in order of the maximum time that each can be down without causing substantial harm to the business. The company must then select a back-up system. In considering which

back-up system to choose, the company should consider the following factors: how quickly the data needs to be restored, how much data must be stored, and how long data must be maintained. It is critical that the company's back-up system be sufficiently segregated from the company's day-to-day systems so that a cyber-attacker cannot access the back-up system during an attack.

Along with the timeline for making back-up systems accessible, the company should implement a plan for replacing essential hardware, and the company should have procedures for testing that the system restore functioned properly. SEC and FINRA rules require regulated entities to establish and regularly test appropriate business continuity protocols.

Manage Relationships with Third-Party Vendors

Relationships with third-party vendors are often necessary. However, those relationships can pose substantial cyber risks that should be mitigated to the extent possible. Vendors should only receive the network access and data necessary to perform their role. The company should scrutinize the adequacy of a third party's cybersecurity policies and procedures before entering into a business relationship with that company. Contractual safeguards should be taken to minimize risk. Vendors should have clear obligations to maintain adequate safeguards to protect sensitive data, and companies should have the right to regularly audit the vendors' compliance. Vendors should be required to notify the company if a breach occurs and the contract should allocate risk in the event that a breach at the vendor harms the company. (Among other things, companies should consider requiring their vendors to carry cyber insurance, and to name the companies as additional insureds.) The company should also consider its interests in controlling the timing and method of any necessary disclosures in the event of a breach. Throughout the business relationship, the company should regularly assess the vendor's security practices and access to the company's data with particular concern for unauthorized access.

Continuously Improve Data Security Policies and Procedures

It is important for companies to regularly measure the effectiveness of their designed solutions, including by revisiting and re-evaluating all of the factors that went into developing them. This applies with equal force to companies' preventive measures, incident response plans, and the business continuity plans. Regular audits should evaluate the companies' compliance with information security policies and the effectiveness of those policies, including conducting tests to ensure that employees are properly and consistently implementing appropriate security measures. Companies that have previously designed and implemented (or do not currently have) privacy and security plans should be mindful of changing laws and regulations, as well as the ever-evolving cyber threats and corresponding best practices.

Engage in Industry Information Sharing

Regulators and lawmakers have recently emphasized that one way for companies to ensure that their data security solutions remain up to date is by participating in industry cybersecurity information sharing. Most recently, on February 13, 2015, President Obama issued an executive order promoting cybersecurity information sharing through the creation of Information Sharing and Analysis Organizations (ISAOs).[5] Companies should actively participate in these information sharing programs. ISAOs allow industry players to keep abreast of evolving cyber-attack tactics and industry security standards. Companies that do not actively participate in industry information sharing risk falling behind in their cybersecurity initiatives and may miss critical information that could prevent or mitigate the consequences of a cyber-event. While some companies may have hesitated to participate in ISAOs in the past due to antitrust concerns, the DOJ and FTC have released a joint statement expressing that "they do not believe that antitrust is – or should be – a roadblock to legitimate cybersecurity information sharing."[6]

Consider Acquiring Cybersecurity Insurance Coverage

The company may also benefit from cybersecurity insurance coverage. Depending on the policy, cyber insurance may cover (i) forensic investigation and system restoration costs; (ii) defense and indemnity costs associated with litigation resulting from the loss of personal information or other sensitive data; (iii) defense costs and penalties associated with regulatory investigations; (iv) notification costs and credit monitoring for affected customers and employees; (v) losses attributable to the theft of the policyholder-company's own data (including transfer of funds); (vi) business interruption costs attributable to a cyber-attack; (vii) costs required to investigate threats of cyber-extortion and payments to extortionists; and (viii) crisis management costs, such as the hiring of public relations firms.

It is critical to carefully review the particular provisions of each cyber liability policy with a broker and coverage counsel. Unlike many traditional policies, cyber liability policies differ significantly because they are not (yet) based on a standard form.

Conclusion

The SEC and FINRA have made clear that they are focused on cybersecurity in the securities industry and this focus is only likely to grow as cyber threats become more sophisticated. Obsolete technical controls, ineffective policies and procedures for company employees, and inadequate detection, response and disclosure of data breaches may all lead to enforcement actions and litigation against regulated entities. Appropriate cybersecurity programs are essential to minimizing regulatory and litigation risk, as well as reputational and other harms. They also lead to better protections against cyber-attacks and less frequent and less severe data breaches. Therefore, a strong cybersecurity program is an essential part of any long-term strategy for regulated entities.

ENDNOTES

1 OCIE Cybersecurity Initiative, April 15, 2014, *available at* http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.

2 New York DFS New Cyber Security Examination Process, December 10, 2014 *available at* http://www.dfs.ny.gov/banking/bil-2014-10-10_cyber_security.pdf.

3 OCIE Cybersecurity Examinations Sweep Summary, February 3, 2015, *available at* http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf; FINRA Report on Cybersecurity Practices, February 3, 2015, *available at* http://www.finra.org/web/groups/industry/@ip/@reg/@guide/documents/industry/p602363.pdf.

4 https://www.fsisac.com/

5 Executive Order – Promoting Private Sector Cybersecurity Information Sharing, February 13, 2015, *available at http://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.*

6 FTC, DOJ Antitrust Policy Statement on Sharing Cybersecurity Information, April 10, 2014, *available at* http://www.justice.gov/atr/public/guidelines/305027.pdf .

This article is reprinted with permission from *Practical Compliance and Risk Management for the Securities Industry,* a professional journal published by Wolters Kluwer Financial Services, Inc. This article may not be further re-published without permission from Wolters Kluwer Financial Services, Inc. For more information on this journal or to order a subscription to *Practical Compliance and Risk Management for the Securities Industry,* go to **pcrmj.com** or call **866-220-0297**