Broker-dealers need to respond to recent focus on cybersecurity threats

Journal of Investment Compliance

By David Petron, Michael Wolk and Edward McNicholas

David Petron, Michael Wolk and Edward McNicholas are partners all based at Sidley Austin LLP, Washington, DC, USA.

Abstract

Purpose – *To alert broker-dealers to several regulatory developments relating to cybersecurity threats.*
Design/methodology/approach – *Reviews four regulatory developments in the cybersecurity area and provides several steps broker-dealers should undertake to review and improve their cybersecurity and information technology protocols and practices.*
Findings – *While FINRA's new cybersecurity sweep appears to be an exploratory and learning exercise to obtain regulatory knowledge and intelligence, firms should be cognizant of the fact that both FINRA and the SEC have imposed significant sanctions against Firms when it has found inadequate cyber security policies and procedures.*
Practical implications – *Broker-dealers should review the White House's recent Framework for Improving Critical Infrastructure Cybersecurity and evaluate their own cybersecurity preparedness under the key areas of the Framework.*
Originality/value – *Practical guidance from experienced privacy and securities regulatory lawyers that consolidates several recent developments in one piece.*
Keywords *USA, Securities and Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA), Broker-dealer, Policies and procedures, Cybersecurity*
Paper type *Technical paper*

Recent data breaches at retailers like Target have increased awareness about growing cybersecurity threats. Broker-dealers in particular need to reevaluate their own cybersecurity preparedness in light of several recent events:

1. FINRA's launch of a cybersecurity sweep, publicly announced on the FINRA website on February 6, 2014.

2. The inclusion of cybersecurity as a priority in the SEC's National Examination Program for 2014 and FINRA's 2014 Annual Regulatory and Examination Priorities Letter.

3. The White House's February 12, 2014 release of the much-anticipated Framework for Improving Critical Infrastructure Cybersecurity.
4. An upcoming SEC public roundtable on cybersecurity issues, to be held in Washington, DC on March 26, 2014.

FINRA cybersecurity sweep

Information technology plays an obviously critical role in the securities industry. In light of the increasing threat to IT systems from numerous sources, FINRA is conducting an assessment of broker-dealers' approaches to managing those threats and protecting their critical IT infrastructure. According to FINRA's public announcement of its new cybersecurity sweep, its goals for the assessment are as follows:

1. To understand better the types of threats that firms face.

2. To increase FINRA's understanding of firms' risk appetite, exposure and major areas of vulnerabilities in their IT systems.

3. To understand better firms' approaches to managing these threats, including through risk assessment processes, IT protocols, application management practices and supervision.

4. As appropriate, to share FINRA's observations and findings with firms.

Public reports suggest that at least 20 targeted sweep letters have already been sent to a diverse group of firms with different business models and potential risk profiles. FINRA's public announcement identified the following cybersecurity areas as included within its assessment: approaches to information technology risk assessment; business continuity plans in case of a cyber-attack; organizational structures and reporting lines; processes for sharing and obtaining information about cybersecurity threats; understanding of concerns and threats faced by the industry; assessment of the impact of cyber-attacks on the firm over the past twelve months; approaches to handling distributed denial of service attacks; training programs; insurance coverage for cybersecurity-related events; and contractual arrangements with third-party service providers.

Cybersecurity as SEC and FINRA examination priority

On February 6, 2014, SEC Chair Mary Jo White testified before the Senate Banking Committee that the SEC's National Examination Program has included cybersecurity issues as a priority for the 2014 examination cycle. Jane Jarcho, the SEC's associate director for the National Examination Program, had previously stated that examiners will focus on policies and resources that are devoted to assessing and responding to cybersecurity risks. SEC examiners can be expected to look into plans and procedures for responding to identity theft, lost information, external and internal cyber attacks, and business continuity.

On January 2, 2014, FINRA in its 2014 Annual Regulatory and Examination Priorities Letter also identified cybersecurity as a priority. FINRA stated that its primary focus is the integrity of firms' policies, procedures and controls to protect sensitive customer data and that its evaluation of such controls may take the form of examinations and targeted investigations.

Framework for improving critical infrastructure cybersecurity

The White House's new Framework for Improving Critical Infrastructure Cybersecurity (the "Framework") was developed by the National Institute for Standards and Technology ("NIST") pursuant to Executive Order No. 13,636 (issued in February 2013). The Framework strongly encourages companies in the financial services and other industries to implement and comply with its voluntary standards. Based in part on input from the private sector, the Framework is intended to provide a procedural framework for assessing practices rather than to establish new substantive standards. According to the White House, the Framework can serve as a cybersecurity roadmap for all companies, providing basic first steps for firms that lack a cybersecurity program, and for firms with existing, advanced programs, offering a concrete method to communicate with executive leaders and third party suppliers to further integrate security practices. The Framework is built on three components. First, the

Framework Core identifies five concurrent functions common across all critical infrastructure entities. All entities should develop the ability to:

1. identify cybersecurity risks and vulnerabilities;

2. protect critical infrastructure assets;

3. detect the occurrence of a cyber event;

4. respond to a detected event; and

5. recover from a cyber event.

Second, the Framework Tiers characterize an entity's cybersecurity practices from partial (Tier 1) to adaptive (Tier 4) compliance. The Tiers are used to assess compliance with the Framework standards and legal and regulatory obligations, and to determine resource allocation. Third, the Framework Profile aligns the Core's standards with the particular needs and practices of an implementation scenario. Companies can compare their current cybersecurity profile with their target profile to assess necessary steps to strengthen security. NIST also published a Roadmap for Improving Critical Infrastructure Cybersecurity, which identified several key areas for improvement in critical infrastructure cybersecurity.

SEC cybersecurity roundtable

On February 14, 2014, the SEC announced that it would hold a March 26 roundtable in Washington on the cybersecurity challenges facing market participants and public companies. The SEC's public announcement noted that "growing interest in cybersecurity across financial markets and other sectors has raised questions about how various market participants can effectively manage cybersecurity threats." The SEC also noted that recent data breaches have focused public attention on these threats. The SEC's roundtable will be open to the public and will be webcast live on the SEC's website. Additional information on the agenda and participants is expected to be publicized in the near future.

What broker-dealers should do now

Broker-dealers should not wait for a FINRA sweep letter or an SEC exam to evaluate their own cybersecurity preparedness. Firms should begin reviewing their cybersecurity and information security protocols now, to assess their practices in light of the new Framework and the regulators' areas of focus. Because it reflects current thinking on cybersecurity best practices, the new Framework provides an excellent tool for firms to begin focusing attention, responsibility and accountability for cybersecurity within their organizations. A good place to start is with reading the actual Framework itself; it is written at a level intended to be fully accessible to non-technical, senior executives.

For next steps, firms should look to NIST's new Roadmap, which provides several key areas for improvement in critical infrastructure cybersecurity, including the following:

_ *Authentication:* improve authentication mechanisms commonly exploited;

_ *Indicator sharing:* develop indicator information for timely and actionable cyber threat detection and response;

_ *Data analytics:* take advantage of the promise of analytic tools applied to big data sources to predict trends and assess weaknesses;

_ *International engagement:* work with foreign governments and international companies to integrate compliance standards around the world;

_ *Supply chain risk management:* integrate cybersecurity standards across vulnerable supply chains; and

_ *Technical privacy standards:* design a privacy risk management model, privacy standards and supporting privacy metrics.

Moreover, while the FINRA sweep appears to be an exploratory and learning exercise to obtain regulatory knowledge and intelligence, firms should be cognizant of the fact that both FINRA and the SEC have imposed significant sanctions against Firms when it has found inadequate cyber security policies and procedures.

Notes

1. Attorney Advertising-For purposes of compliance with New York State Bar rules, our headquarters are Sidley Austin LLP, 787 Seventh Avenue, New York, NY 10019, 212.839.5300; One South Dearborn, Chicago, IL 60603, 312.853.7000; and 1501 K Street, N.W., Washington, D.C. 20005, 202.736.8000.
2. Sidley Austin provides this information as a service to clients and other friends for educational purposes only. It should not be construed or relied on as legal advice or to create a lawyer-client relationship. Prior results do not guarantee a similar outcome.

Corresponding author
David Petron can be contacted at: dpetron@sidley.com

DOI 10.1108/JOIC-05-2014-0020 VOL. 15 NO. 2 2014, pp. 29-32, Emerald Group Publishing Limited, ISSN 1528-5812 JOURNAL OF INVESTMENT COMPLIANCE