Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

SEC Cybersecurity Findings May Establish De Facto Standard

Law360, New York (February 04, 2015, 5:24 PM ET) --

Alexander H. Southwell

On Feb. 3, 2015, the U.S. Securities and Exchange Commission released a risk alert with summary observations of results from the Office of Compliance Inspections and Examinations' assessment of select regulated entities' cybersecurity efforts. Because of the considerable number of firms reporting the implementation of comparable cybersecurity measures, these findings may further establish a baseline for an emerging standard against which industry participants' conduct can be measured in litigation and regulatory matters. Accordingly, firms should consider implementing minimum requirements, such as those outlined in section 3 below.

1. The Cybersecurity Examination Initiative

In April 2014, the OCIE announced that it would conduct examinations of a sample of registered broker-dealers and registered investment advisers to assess their cybersecurity practices and preparedness (the "cybersecurity examination initiative"). This initiative came in the wake of the March 26, 2014, SEC-sponsored Cybersecurity Roundtable, which was held to discuss growing cybersecurity threats and provide the SEC with information to evaluate what additional steps the SEC should take to address cybersecurity threats to regulated entities.

The examinations were to focus on: "the entity's 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 experience with certain cybersecurity threats."[1]

The risk alert announcing the cybersecurity examination initiative also included an appendix containing a sample request for information to guide firms in responding to the examinations or, for those firms not examined, in assessing their own cybersecurity preparedness.

The SEC's summary of the 2014 examinations covers 57 registered broker-dealers and 49 registered investment advisers, which were "selected to provide perspectives from a cross-section of the financial services industry and to assess various firms' vulnerability to cyberattacks."[2] The summary includes

information collected and analyzed from documents and from interviews with personnel serving in key positions at these firms.

2. The Findings

The SEC summary of the cybersecurity examination initiative reported that certain cybersecurity practices are widespread among the firms examined. For example, written information security policies have been adopted by most of the studied firms — 93 percent of examined broker-dealers and 83 percent of examined advisers. Most of the broker-dealers (89 percent) surveyed conduct periodic compliance audits for these policies, although the number of advisers conducting these audits is lower at 57 percent.

A similar proportion of the firms — 88 percent of broker-dealers and 53 percent of advisers — model their cybersecurity processes after external standards, including those published by the National Institute of Standards and Technology, the International Organization for Standardization, and the Federal Financial Institutions Examination Council. Many firms also include plans for mitigating a cybersecurity incident's effects or recovering from such an incident (82 percent of broker-dealers and 51 percent of advisers).

The vast majority of firms also undertake firmwide risk assessments to identify cybersecurity threats, vulnerabilities and potential business consequences. Ninety-three percent of broker-dealers and 79 percent of advisers considered these risk assessments in establishing their cybersecurity procedures.

Other best practices reported by firms included:

- Use of encryption in some form (98 percent of broker-dealers and 91 percent of advisers);

- Designation of a chief information security officer (68 percent of broker-dealers, but only 30 percent of advisers);

- Use of cybersecurity insurance for losses and expenses attributable to cybersecurity incidents (58 percent of broker-dealers and 21 percent of advisers);

- Identification of best practices through information-sharing networks, such as industry groups, associations or organizations that exist for the purpose of sharing information regarding cybersecurity (the approach taken by roughly a majority of broker-dealers) or relying on discussions with industry peers, attending conferences and conducting independent research (the preferred approach of advisers); and

- Firmwide inventorying, cataloging, or mapping of technology resources. The reported use of this assessment varied by the type of resource, but nearly all broker-dealers and at least a solid

majority of advisers apply such processes to the following: physical devices and systems; software platforms and applications; network resources, connections and data flows; connections to firm networks from external sources; hardware, data and software; and logging capabilities and practices.

Most of the entities surveyed also reported that they had been the subject of a cybersecurity incident. Cyberattacks were experienced either directly or through one or more vendors by 88 percent of broker-dealers and 74 percent of advisers. Of these attacks, the majority were reported to be due to malware and fraudulent emails.

About half of the firms (54 percent of broker-dealers and 43 percent of advisers) indicated that they received fraudulent emails seeking to transfer client funds. Of those broker-dealers reporting losses to fraudulent emails, 25 percent indicated that the losses resulted from a failure of employees to follow the firms' identity authentication procedures.

Although firms indicated concern about misconduct by employees or other authorized network users, only 11 percent of broker-dealers and 4 percent of advisers reported misconduct by these individuals that resulted in misappropriation of funds, securities, sensitive client or firm information, or damage to the firm's network.

Interestingly, while some cybersecurity practices by firms are widespread and the incidents of cyberattacks were also widely reported, a smaller proportion of firms reported requiring third parties with which they interact to implement cybersecurity requirements. Although 84 percent of broker-dealers reported applying requirements for periodic risk assessments to their vendors, only 32 percent of advisers required such assessments.

Similarly, 72 percent of broker-dealers and only 24 percent of advisers reported integrating requirements relating to cybersecurity risk into vendor and business partner contracts. Even fewer firms reported maintaining policies and procedures on information security training for vendors and business partners authorized to access the firms' networks (51 percent of broker-dealers and only 13 percent of advisers). But, it should be noted that this assessment was conducted beginning in April 2014, before the recent series of high-profile cybersecurity breaches. It is likely that more firms are now paying attention to third-party risks with regard to network access and breaches.

Additionally, more firms provide their clients with suggestions regarding information protection. All of the reporting broker-dealers that offer online access to retail customers provide customers with some form of information on how to reduce cybersecurity risks associated with transactions with the firm. A majority (75 percent) of advisers with retail clients that can access their account information online also provide clients with information about reducing cybersecurity risk in transactions.

Also on Feb. 3, 2015, the Financial Industry Regulatory Authority released its own report on cybersecurity practices based on its 2014 targeted examination of a cross section of firms, including investment banks, clearing firms, online brokerages, high-frequency traders and independent dealers. The FINRA report identifies many of the same principles and practices highlighted in the OCIE's cybersecurity examination initiative results, and provides detailed discussions of firm practices.

3. The Way Forward

The OCIE cybersecurity examination initiative focused on a small sampling of firms, given that the OCIE is responsible for examining approximately 4,500 registered broker-dealers and over 10,000 registered investment advisers. However, the results of the cybersecurity examination initiative and the FINRA report may nonetheless have considerable impact in terms of shaping emerging best practices related to cybersecurity.

The broad consensus that emerges from these findings suggests that companies housing confidential proprietary materials, and more specifically, those in the financial services industry, should consider this data in devising, assessing and improving their own internal cybersecurity and compliance programs. Among the practices to consider are the following:

1. Draft or update written information security policies and procedures, including continuity or response plans, and consider requiring third-party vendors to disclose their policies as a condition of engagement.

2. Identify and consider implementation of best cybersecurity practices, such as use of encryption and a defense-in-depth strategy, and possible emerging industry standards of care through industry groups, associations, conferences, and existing published guidance from regulators and government agencies.

3. Review existing risk assessment and corporate governance mechanisms as they relate to cybersecurity and revise these mechanisms to address cybersecurity risks, which may include adopting the NIST Cybersecurity Framework.

4. Implement firmwide risk assessments on a regular basis to identify cybersecurity threats, vulnerabilities and potential business consequences, and consider requiring third-party vendors to do the same as a condition of engagement.

5. Review and assess employee guidelines concerning cybersecurity, email, confidentiality, and third-party identity authentication procedures, penalties for lack of adherence thereto, and enforcement mechanisms in support of such policies.

6. Consider designating a chief information security officer for cybersecurity oversight and accountability.

7. Educate appropriate personnel concerning industry-specific reporting guidelines, if any, for cybersecurity breaches.

8. Implement, assess and monitor firmwide inventorying of technology resources.

9. Evaluate the need for, and potential coverage afforded by, cybersecurity insurance.

While the cybersecurity examination initiative does not create a regulatory mandate regarding cybersecurity, it provides valuable insight into what may be evolving industry best practices and consensus on reasonable efforts relating to cybersecurity. Accordingly, organizations, particularly those within the financial services industry, should review the SEC findings and the FINRA report, as well as pertinent industrywide standards.

Additionally, key security personnel should be engaged to assess the feasibility of implementing specific technical processes, and legal counsel should advise appropriate company leadership about the risks involved in adopting or foregoing implementation of critical best practices.

Organizations should consider implementing the measures identified above as determined to meet specific company's requirements and regulatory obligations (as in the case of 31 C.F.R. § 1023.320(a)(2)'s reporting requirement, for example). However, companies should be aware that industrywide adoption of discretionary measures could lend itself to establishment of a de facto standard of care against which potential liability may be measured in both the litigation and regulatory context. For this reason, firms choosing not to establish similar baseline minimum standards could potentially be held liable for loss if it is determined that a minimum standard of care exists.

—By Alexander H. Southwell, Angelique Kaounis, Stephenie Gosnell Handler and Zachary Wood, Gibson Dunn & Crutcher LLP

Alexander Southwell is a partner in Gibson Dunn's New York office. Angelique Kaounis is of counsel in the firm's Century City office in Los Angeles. Stephenie Gosnell Handler is an associate in Washington, D.C. Zachary Wood is an associate in the firm's Palo Alto, California, office.

[1] SEC Office of Compliance Inspections and Examinations, OCIE Cybersecurity Initiative, Risk Alert (April 15, 2014), available at http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.

[2] SEC Office of Compliance Inspections and Examinations, Cybersecurity Examination Sweep Summary, Risk Alert (Feb. 3, 2015), available at http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.