The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 28780

February 26, 2015

FINRA Publishes a Report on Members' Cybersecurity Practices That Discusses Recommended Principles and Effective Practices

[28780]

February 26, 2015

TO: SEC RULES MEMBERS No. 14-15
COMPLIANCE MEMBERS No. 9-15
SMALL FUNDS MEMBERS No. 9-15
TECHNOLOGY COMMITTEE No. 4-15
CHIEF INFORMATION SECURITY OFFICER ADVISORY COMMITTEE
BROKER/DEALER ADVISORY COMMITTEE No. 8-15
TRANSFER AGENT ADVISORY COMMITTEE No. 9-15
OPERATIONS MEMBERS No. 8-15
PRINCIPAL UNDERWRITERS WORKING GROUP
CHIEF RISK OFFICER COMMITTEE No. 5-15
INTERNAL AUDIT ADVISORY COMMITTEE No. 3-15 RE: FINRA PUBLISHES A REPORT ON MEMBERS' CYBERSECURITY PRACTICES THAT DISCUSSES RECOMMENDED PRINCIPLES AND EFFECTIVE PRACTICES

Earlier this month, FINRA published a 46-page report on its members' cybersecurity practices. [1] Some of the information in the Report came from information gathered during FINRA's 2014 targeted examination of its members' cybersecurity practices. According to FINRA, a variety of factors, including advances in technology, changes in the firms' business models, and changes in how firms and their customers use technology, create vulnerabilities in firms' information technology systems and may expose them to cybersecurity threats. The Report identifies principles and effective practices for members to consider to develop cybersecurity programs that both are grounded in risk management and address evolving threats. It presents key points and provides information on select topics in order to provide a resource for firms developing or advancing their cybersecurity programs. The areas discussed in the Report are briefly descried below.

Key Points of the Report

As stated in the Report, "FINRA's objective is to focus firms on a risk management-based approach to cybersecurity." [2] It defines "cybersecurity" broadly as "the protection of investor and firm information from compromise through the use – in whole or in part – of electronic digital media (e.g., computers, mobile devices or internet protocol-based telephony systems)." As used in this definition, "compromise" refers to a loss of data confidentiality, integrity, or availability. [3] The Report discusses the results from sweeps conducted by FINRA in 2011 and 2014 in which members listed as their top three threats: hackers penetrating their systems; insiders compromising firm or client data; and operational risks. With respect to members' overall threat environment, the Report notes that the ranking of threats reported by members varies by firm and business model (e.g., online brokerage firms are more likely to list hackers as a top priority). To inform its cybersecurity program, a firm needs to understand the threats it faces, its assets most likely to be targeted for attack, and the likely source of these threats.

Topics Addressed in the Report

The Report discusses principles and effective practices in eight areas. Its discussion of these issues includes observations on firm practices from FINRA's 2014 review. These areas are as follows: [4]

1. Governance and Risk Management for Cybersecurity – According to the Report, firms should establish and implement a cybersecurity framework that supports both informed decision making and escalation within the organization to identify and manage cybersecurity risks. The framework should include defined risk management policies, processes, and structures coupled with relevant controls tailored to the nature of the cybersecurity risks the firm faces and its resources. [5]

2. Cybersecurity Risk Assessment – The Report encourages firms to conduct regular assessments to identify cybersecurity risks associated with firm assets and vendors and prioritize their remediation. As part of this process, firms should inventory their assets and know which of their assets are critical. The Report suggests steps a firm can take to establish and maintain a risk assessment program. [6]

3. Technical Controls – The Report next discusses the importance of firms implementing technical controls to protect firm software and hardware that stores and processes data, as well as the data itself. These controls might include: multi-layer defenses, identity and access management, authorization and entitlement protocols, encryption, and third-party penetration testing. [7]

4. Incident Response Planning – According to FINRA, firms should establish policies and procedures, as well as roles and responsibilities, for escalating and responding to cybersecurity incidents. Effective practices in this area might include: anticipation of the types of events the firm may encounter; consideration of containment and mitigation strategies; investigation and damage assessment processes; participation in industry and firm simulations; and implementation of measures to maintain client confidence (e.g., providing credit monitoring in the event of a breach or reimbursement of financial losses). [8]

5. Vendor Management – The Report discusses the importance of firms managing cybersecurity risks that can arise across the lifecycle of vendor relationships. In

addition to using a risk-based approach to vendor management, other practices to manage vendors might include pre-contract and ongoing due diligence, establishing contractual terms appropriate for the information and systems accessible to the vendor, and processes to terminate vendor access upon termination of a relationship, among others. [9]

6. Staff Training – According to the Report, firms should provide cybersecurity training to staff and such training should be specifically tailored to the staff's needs. To do so, firms may want to identify training requirements and cycles, deliver interactive training with audience participation (to increase retention), and incorporate firm-specific information into the training. [10]

7. Cyber Intelligence and Information Sharing – The Report recommends that firms use cyber threat intelligence to improve their ability to identify, detect, and respond to cybersecurity threats. Effective practices in this area might include: assigning responsibility for this at both organizational and individual levels; establishing mechanisms to promptly distribute threat information to appropriate persons; evaluating threat information both tactically and strategically; and participating in appropriate information sharing organization (such as FS-ISAC). [11]

8. Cyber Insurance – Finally, the Report recommends that firms evaluate the utility of cyber insurance as a way to transfer some of their risk. For those firms that already have such insurance, the Report recommends that they periodically assess its adequacy in light of the firms' changing risk profile. For those firms that do not currently have such insurance, the Report recommends that they evaluate whether coverage is available that would help them manage the financial impact of cybersecurity events. [12]

The Report concludes by stating that "FINRA expects that firm management will make cybersecurity a priority and that it will devote sufficient resources both to understand the current and evolving cybersecurity threats to which the firm may reasonably expect to be exposed and to implement measures necessary to achieve the desired risk posture." [13]

Tamara K. Salmon
Associate General Counsel

endnotes

[1] See Report on Cybersecurity Practices, A Report from the Financial Industry Regulatory Authority, FINRA (February 2015) ("Report"), which is available at http://www.finra.org/web/groups/industry/@ip/@reg/@guide/documents/industry/p602363.pdf.

[2] Report at p. 3.

[3] Report at p. 3.

[4] Each of these areas and effective practices members may want to consider in connection with them, are discussed in detail in the Report. The Report also includes three appendices – the first summarizes the Report's Principles and Effective Practices (pp. 39-41); the second contains the NIST Framework (pp. 42-44); and the third contains a brief discussion of encryption considerations (p. 45).

[5] See pp. 6-11. This discussion notes that firms can draw upon various standards or frameworks to use as reference points in developing their cybersecurity programs. These resources include NIST and the SANS Top 20.

[6] See pp. 12-15.

[7] Report at pp.16 -23. As noted above, Appendix III to the Report (p. 45) discussed encryption considerations.

[8] Report at pp. 23-25.

[9] Report at pp. 26-30.

[10] Report at pp. 31-33.

[11] Report at pp. 34-36.

[12] Report at pp. 37-38.

[13] Report at p. 38.
