WINSTON & STRAWN LLP

CLIENT ALERT

The SEC and FINRA Issue Investor Bulletins and Reports on Cybersecurity

FEBRUARY 19, 2015

On February 3, 2015, the SEC and FINRA each issued investor bulletins and reports on cybersecurity – an area of concern that seems to take on added urgency with each passing week. See SEC Press Release and FINRA Press Release. Both the SEC Investor Bulletin, titled "Protecting Your Online Brokerage Accounts from Fraud," which was written by the SEC's Office of Investor Education and Advocacy, and FINRA's Investor Alert, titled "Cybersecurity and Your Brokerage Firm," were written for the benefit of the investing public. These publications generally encourage investors to understand their firm's cybersecurity policies and include advice to help investors safeguard their accounts and personal financial information.

The SEC's Risk Alert, which was published by the SEC's Office of Compliance Inspections and Examinations ("OCIE"), summarizes OCIE's recent examination sweep of 57 broker-dealers and 49 investment advisers. These examinations focused on how firms identify cybersecurity risks; establish cybersecurity policies, procedures, and oversight processes; protect their networks and information; identify and address risks associated with remote access to client information, funds transfer requests, and third-party vendors; and detect unauthorized activity. Helpfully, the SEC's Risk Alert also provides percentage breakdowns of the number of broker-dealers and advisers that engaged in the various practices highlighted in the Alert.

FINRA's Report on Cybersecurity Practices takes a different approach from the SEC's Risk Alert. Rather than summarizing the results of its recent cybersecurity sweep exams, FINRA's Report instead provides "an approach to cybersecurity grounded in risk management" that is particularly substantive and sets forth "principles and practices for firms to consider". FINRA's Report is useful not only to FINRA's member firms but to any financial services company. Topics covered by FINRA's report include cybersecurity risk assessment, technical controls, incident response planning, vendor management, staff training, cyber intelligence and information sharing, and cyber insurance.

The most significant item in FINRA's Report, however, is its focus on the importance of a strong governance framework. The term "governance framework" is used by FINRA to refer broadly "to the establishment of policies, procedures and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements in a fashion that is understood within the organization and that informs its management of cybersecurity risk." Indeed, FINRA's Report highlights the importance of a sound governance framework by listing it

as the first key point in the Report. We agree with FINRA that a strong governance framework is instrumental in creating a firm foundation for a cybersecurity program, thereby contributing significantly to its success.

From a compliance perspective, however, an effective cybersecurity program is only half the battle. A regulated financial services firm must be able to demonstrate to regulators that it has an effective cybersecurity program. We believe that the key to being able to make this demonstration lies in following the governance framework described in FINRA's Report. That is, not only will a strong governance approach make for a better cybersecurity program but, importantly, it will also lead to cybersecurity program documentation that is both consistent with the expectations of FINRA and the SEC, and allow for easier and more effective communications with the regulators around this difficult topic.

This is true of routine regulatory responses – FINRA member firms should expect cybersecurity preparedness reviews as part of every routine regulatory examination. It is equally true of responses to regulatory inquiries that are triggered by incidents or other demonstrated weaknesses, in which case, documentation of a strong governance framework is likely to lessen the severity of any action taken by FINRA or the SEC and hopefully ward off charges against individuals.

An outline of the governance framework described in FINRA's report is set forth below. While we believe this outline will be helpful to firms in their own efforts to prepare an appropriate governance framework, we recommend that firms not rely exclusively on this outline and that they carefully review the entire Report. In addition, any framework adopted should, of course, be tailored to the specific circumstances at hand. That is, there is no one-sized fits all solution.

Governance Framework Outline

Based upon FINRA's Report on Cybersecurity Practices (Feb. 2015)

Formation of a Cybersecurity Committee or Working Group.
The creation of a cybersecurity committee or working group is the starting point for any governance framework. This outline uses the term "Cybersecurity Committee" for that purpose. The Cybersecurity Committee should be tasked with:

- responsibility at a high level for the firm's cybersecurity policies and procedures;
- reporting to senior management and the board (full board or audit or other committee) on a periodic basis and upon the happening of material events; and
- monitoring the firm's cybersecurity program through the receipt of periodic and event driven status updates and other reports by designated officers and possibly consultants or other third parties as to the function of the firm's cybersecurity program.

Composition of the Cybersecurity Committee.
Firms should ensure that the committee members collectively have sufficient authority, expertise, and independence. Committee members are likely to include representatives from business, information technology, risk management and internal audit.Committee members may also include legal and compliance members.

Required Documentation.
Recommended required documentation includes:

- written committee charter
- minutes reflecting committee considerations and actions
- written policies and procedures governing responsibilities of the Cybersecurity Committee and responsibilities of officers within the firm with respect to the firm's cybersecurity program

Tasks to be Covered by Policies and Procedures.
The policies and procedures specific to the Cybersecurity Committee should identify, in detail, the Committee's monitoring and reporting functions, including the Committee's responsibility to ensure that it has taken reasonable steps to ensure its receipt of any required reports or other communications. The Committee's policies and procedures should also provide for the assignment to identified officers within the firm or third parties of the following tasks, including the development of procedures related to such tasks:

1. Risk Assessment. The completion of an initial risk assessment and, thereafter, the performance of additional risk assessments on both a periodic and an event driven basis, i.e., in response to change in business or technology, material failure or identification of a material weakness or other red flags indicating the need for improvements.

   The risk assessment process requires the identification of a relevant industry framework and standards and must be conducted by a team that has the necessary independence, expertise, and authority for the task.

   Simplistically, the risk assessment process can be thought of as including three steps:

- Identification of risks, *e.g.*, protection of customer and sensitive data, the misuse of customer funds or securities, and the theft of proprietary algorithms, including the identification of the location of assets, e.g., customer data, and whether such assets are authorized to be on a firm's network.
- Weighing the severity of the identified risks, i.e., what assets are most important to protect.
- Identifying a process to manage and monitor identified risks. FINRA describes management's choices in this regard as avoid, accept, mitigate or transfer through insurance.
  - Mitigation incudes identification, selection, implementation, performance monitoring (day to day and supervision thereof), and updating.
  - Implementation can include a variety of controls, including preventive, detective, corrective, and event predictive, i.e., based upon notifications or awareness of issues at other firms.

2. Establishment of controls, restrictions and monitoring relating to information creation, storage and access.

3. Establishment of a change control process designed to ensure that new processes, equipment, vendors, material changes in business, etc. are covered by the firm's cybersecurity program.

4. Vendor due diligence and oversight.

5. Establishments of performance metrics and escalation policies.

6. Periodic independent audit of implementation and effectiveness.

7. Establishment of staffing and budget requirements.

8. Establishment of an Incident Response Plan, including considerations regarding:

- internal notifications, including Cybersecurity Committee, legal, compliance,
- regulatory and law enforcement notifications, including SARs
- customer notification

9. Establishment of a training program.

10. Establishment of a reporting framework up to the Committee and from the Committee to senior management and the board. These procedures should specify the information that will be reported to the Committee and that the Committee will report to senior management, the board, and/or legal and compliance. The Committee should require that it be informed of significant incidences on an ongoing basis and should obtain periodic reports from key officers. Reporting to senior management and the board by the Committee should be both periodic and event driven.

11. Participation in industry and other groups. The procedures should provide for participation in industry or other groups for the purposes of sharing best practices and concerns.

6 Min Read

Related Locations

Charlotte | Chicago | Houston | Los Angeles | New York | San Francisco | Silicon Valley | Washington, DC

Related Topics

Financial Services | Corporate | FINRA | Securities and Exchange Commission (SEC)

Related Capabilities

Transactions | Financial Services Transactions & Regulatory | Financial Services

Related Regions

North America

Related Professionals

Basil Godellas