SEC and FINRA Issue Results of Cybersecurity Examinations

Wednesday, February 18, 2015

On February 3, 2015, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert providing summary observations derived from the staff's sweep examinations of over 100 registered broker-dealers and investment advisers that were undertaken to assess the cybersecurity practices and preparedness of such firms (the Cybersecurity Examination Initiative). On the same day, FINRA published a detailed, 46-page Report on Cybersecurity Practices identifying effective practices for dealing with cybersecurity threats, a product of its own 2014 targeted examinations of member firms and related initiatives, including a 2011 cybersecurity survey of its registered broker-dealers.

OCIE Risk Alert

In implementing the Cybersecurity Examination Initiative, OCIE staff interviewed key personnel and evaluated information and materials from 57 registered broker-dealers and 49 registered investment advisers relating to the firms' practices for: identifying cybersecurity-related risks; establishing cybersecurity governance, including policies, procedures and oversight processes; identifying and responding to risks relating to service providers, vendors and other third parties; safeguarding network infrastructure and information; identifying and managing risks associated with remote access to client information and funds transfer requests; and uncovering unauthorized activity. The Risk Alert states that the staff's inquiries and document reviews were "designed to discern basic distinctions among the level of preparedness of the examined firms."

Notable observations in the Risk Alert include (figures pertain to examined firms):

- 88% of broker-dealers and 74% of investment advisers reported cyber attacks directly or through one or more vendors, the majority of which arose from malware and fraudulent e-mails.

- 93% of broker-dealers and 83% of the investment advisers have adopted written information security policies.

- The written information policies and procedures of "only a small number" of broker-dealers (30%) and investment advisers (13%) contain provisions addressing how firms determine whether they are responsible for client losses associated with cyber incidents; even fewer of the broker-dealers (15%) and advisers (9%) offer security guarantees to protect clients against losses related to such incidents.

- 88% of the broker-dealers and 53% of the investment advisers reference and/or incorporate published cybersecurity risk management standards in their information security policies, such as those of the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO) and the Federal Financial Institutions Examination Council (FFIEC).

- The "vast majority" of the broker-dealers (93%) and investment advisers (79%) conduct periodic risk assessments on a firm-wide basis to detect cybersecurity threats, weaknesses and potential business consequences, and they use these assessments to establish their cybersecurity policies and procedures.

- Although most of the broker-dealers (84%) require cybersecurity risk assessments of vendors with access to their systems, a "small number" (15%) make any attempt to verify the service providers' security posture, as part of their overall risk management programs.

- In evaluating the back-up and disaster recovery procedures for cybersecurity threats, the staff found that 88% of broker-dealers and 53% of investment advisers reported that they maintain such procedures, though the written policies and procedures of a "small number (30%) of broker-dealers and 13% of investment advisers" describe these procedures in a manner that does not include any technical or operational detail.

- 88% of the broker-dealers and 53% of the investment advisers report that they have in place procedures to address potential risks from third-party providers, though again, the written policies and procedures of a "small number" of broker-dealers (30%) and investment advisers (13%) do not adequately describe these procedures.

- The staff observed that 67% of broker-dealers and 26% of investment advisers maintain written procedures relating to third-party providers, though the "vast majority" of the broker-dealers (93%) and investment advisers (79%) report that they use cybersecurity risk assessments to evaluate the risk posed by third-party providers.

- The written policies and procedures of 30% of broker-dealers and 13% of investment advisers describe procedures relating to the cybersecurity controls of third-party providers, and many of these procedures are not adequately documented in the firms' written policies and procedures.

- The staff observed that 93% of broker-dealers and 79% of investment advisers report that they have in place written procedures relating to third-party providers, though the written policies and procedures of 30% of broker-dealers and 13% of investment advisers describe these procedures in a manner that does not include any technical or operational detail.

- The staff observed that 93% of broker-dealers and 79% of investment advisers report that they have in place written procedures relating to third-party providers, though the written policies and procedures of 30% of broker-dealers and 13% of investment advisers describe these procedures in a manner that does not include any technical or operational detail.

- The staff observed that 93% of broker-dealers and 79% of investment advisers report that they have in place written procedures relating to third-party providers, though the written policies and procedures of 30% of broker-dealers and 13% of investment advisers describe these procedures in a manner that does not include any technical or operational detail.
to their firms’ networks, only 32% of the advisers have such requirements for vendors. A large majority (72%) of the broker-dealers incorporate requirements relating to cybersecurity in vendor contracts, but only 24% of investment advisers do so.

- Almost all broker dealers (98%) and investment advisers (91%) make use of data encryption in some form.
- A majority (58%) of broker-dealers maintain insurance that covers losses and expenses attributable to cybersecurity incidents, but only 21% of investment advisers do so.

The Risk Alert focuses more on the existence of cybersecurity controls rather than their quality, noting that the exams “did not include reviews of technical sufficiency of the firms’ programs.” The Alert cautions that OCIE staff is “still reviewing the information [obtained in the sweep exams] to discern correlations between the examined firms’ preparedness and controls and their size, complexity or other characteristics.”

OCIE announced the Cybersecurity Examination Initiative on April 15, 2014, in a Risk Alert accompanied by a sample request for information and documents. The announcement of the Cybersecurity Examination Initiative followed the SEC Cybersecurity Roundtable on March 26, 2014. OCIE also listed cybersecurity preparedness in its 2014 examination priorities.

FINRA Report on Cybersecurity Practices

FINRA’s 2014 cybersecurity examination of registered broker-dealers had four primary objectives: (i) to better understand the types of cybersecurity threats that are relevant to firms; (ii) to increase understanding of “firms’ risk appetite, exposure and major areas of vulnerabilities in their information technology systems”; (iii) to assess firms’ processes and procedures for managing these threats; and (iv) to share observations and findings with member firms.

FINRA sought information from a cross section of firms, including investment banks, clearing firms, online brokerages, high-frequency traders and independent dealers. FINRA's sweep examinations do not reflect a new regulatory focus; as noted in the FINRA Report, “[c]ybersecurity has...been a regular theme in [FINRA's] Regulatory and Examination Priorities Letter since 2007.” FINRA conducted a survey of 224 member firms in June 2011 to “better understand industry information technology and cybersecurity practices and issues that may impact investor protection or market integrity.” FINRA also conducted on-site review of firms in 2010 and 2011 to provide a better understanding of how firms manage critical information technology and cyber threats.

The FINRA Report is the product of these efforts. The Report provides detailed discussions of firm practices using selected case studies, and offers critical guidance for firms to develop or advance their cybersecurity programs in light of the “threat landscape,” in particular the three top cybersecurity threats identified by broker-dealers: hackers attempting to penetrate firm systems, insiders compromising firm or client data, and operational risks.

The Report lists key principles and effective cybersecurity practices, including the following:

- Firms should have a sound governance framework with sound leadership, including direct engagement by board-level and senior-level management on cybersecurity issues.
  - The framework should include defined risk management policies, processes and structures with controls tailored to the firm's risks and available resources.
- Firms should conduct regular, comprehensive risk assessments of cybersecurity threats they face, including external and internal threats and asset vulnerabilities.
  - Firms should identify and maintain an inventory of assets that are authorized to access the firm's network.
  - Firms should recommend and implement steps to remediate identified risks.
- Firms should use technical controls to protect firm software and hardware based on the circumstances of the firm. Controls may include identity and access management, data encryption and penetration testing.
  - Firms should implement a defense-in-depth strategy, in which the firm strategically layers multiple independent security controls throughout its information technology systems.
- Firms should develop, implement and test incident response plans, and assign staff roles and responsibilities for responding to cybersecurity incidents.
Appropriate response plans should include strategies for containment and mitigation, eradication and recovery for systems and data, investigation and damage assessments processes, and notification to interested parties.

- Firms should incorporate strong due diligence procedures throughout the life cycles of relationships with vendors who access sensitive firm or client information.
  - Firms should conduct pre-contract due diligence on prospective vendors, and use contract terms that establish the vendor’s obligations during and after the vendor’s relationship with the firm.
  - Firms should perform ongoing due diligence on existing vendors.
  - Vendor relationships and outsourced systems should be made a part of the firm's risk assessment process.
  - Firms should establish and implement procedures to terminate vendor access to the firm's systems promptly upon contract termination.

- Firms should train staff to reduce the probability of cyber attacks, using information from the firm's loss incidents, risk assessment process, and threat intelligence gathering.

- Firms should collaborate through intelligence-sharing opportunities to protect the industry from cyber threats.
  - Each firm should assign specified personnel with the responsibility to gather and analyze cybersecurity intelligence.
  - Firms should establish mechanisms to quickly communicate threat intelligence and analysis to appropriate groups within the firm.
  - Firms should participate in information-sharing organizations such as the Financial Services Information Sharing Intelligence and Analysis Center (FS-ISAC), and periodically evaluate the firm's information-sharing partners.

- Firms should establish and implement procedures to terminate vendor access to the firm's systems promptly upon contract termination.

The breadth and detail of the FINRA Report and OCIE's Risk Alert underscore growing concern over cybersecurity threats faced by regulated broker-dealers and investment advisers. Although many firms have taken significant steps directed at mitigating cybersecurity threats, firms should carefully evaluate their cybersecurity policies and practices and implement changes in light of these releases.

In particular, firms should evaluate whether firm policies and procedures adequately cover the following steps consistent with the firm's risk assessment, resources and other circumstances:

1. Periodic Risk Assessments
   - Identify potential cybersecurity threats (including physical security threats) to security, confidentiality and integrity of personal and other sensitive information (both customer and internal), and related systems.
   - Evaluate effectiveness of current controls in light of identified risks.
   - Prioritize resources, assets and systems corresponding to the nature and level of threats and vulnerabilities; revise procedures and controls as warranted to address and mitigate material risks.
   - Determine whether existing insurance policies cover anticipated threats identified in the risk assessment, and determine whether separate cyber coverage is needed.

2. Third-Party Vendor Risks
   - The firm should closely research and evaluate third-party vendors, preferably before they are engaged and periodically thereafter. Review due diligence procedures for selecting vendors, and procedures to approve and monitor vendor access to firm networks, customer data and other sensitive information.
   - Obtain copies of the vendors' written information security plans and certifications of compliance with...
applicable standards.

- Determine whether vendor contracts include appropriate terms on security measures, including incident response notification procedures and cyber insurance coverage.

3. Develop and Periodically Test a Comprehensive Incident Response Plan

- Implement a comprehensive written incident response plan to respond to actual or suspected cybersecurity events. The plan should outline incident reporting mechanisms, circumstances that may warrant outside legal and forensic experts, and notifications to affected individuals, law enforcement, regulators, media or other third parties.

- Conduct periodic "tabletop" exercises of mock cybersecurity events with IT, legal, compliance, human resources and other staff.

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


3 Appendices to the Risk Alert provide breakdowns of the types of broker-dealers and advisers examined. Notably, of the total assets under management of the investment advisers examined, only 2% was accounted for by registered investment companies they advise, with the majority of clients categorized as "Diversified/Institutional."

4 Risk Alert at 1.

5 Id. at 2.

6 Id.

7 Id. at 5

8 Id.

9 FINRA Report at 3.

10 Id.

11 Id.

© 2019 Vedder Price

Source URL: https://www.natlawreview.com/article/sec-and-finra-issue-results-cybersecurity-examinations