WILMERHALE

SEC Issues Cybersecurity Examination Risk Alert

9/18/2015

On September 15, the Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert re-emphasizing the careful scrutiny it will give to the data security practices of broker-dealers and investment advisers and describing areas of particular interest.[1] Those areas include: (i) governance and risk assessment, (ii) access rights and controls, (iii) data loss prevention, (iv) vendor management; (v) training, and (vi) incident response. According to OCIE, the Risk Alert should enable firms to assess whether enhancements to their supervisory, compliance and risk management processes are necessary.

The Appendix to the Alert includes a quite specific list of information requests registered firms are likely to face,[2] drawing on the Framework for Improving Critical Infrastructure Cybersecurity issued by the National Institute of Standards and Technology (NIST) in 2014.[3] Firms should carefully review the Appendix and use it as a self-assessment guide.

This Risk Alert represents the latest step in the SEC's and FINRA's heightened attention to cybersecurity. In April 2014, OCIE issued a Risk Alert announcing steps to assess the cybersecurity preparedness of more than 50 registered broker-dealers and investment advisers. FINRA also conducted targeted sweeps in 2014. On February 3, 2015, both the SEC and FINRA released reports summarizing the results of their cybersecurity sweeps.[4]

2015 Risk Alert Focus Areas

The six areas of particular concern identified in OCIE's Risk Alert are as follows:

Governance and risk assessment: Examiners may assess whether a firm has a tailored cybersecurity governance and risk assessment framework. Examiners may also assess whether a firm's cybersecurity program includes periodic evaluations of cybersecurity risks and engages the firm's senior management and board of directors.

Access rights and controls: Examiners may assess a firm's user access and system authorization controls (including the controls associated with remote access, customer logins, passwords, firm protocols to address customer login problems, network segmentation and tiered access).

1. Data loss prevention: Examiners may assess a firm's processes to monitor potentially

unauthorized data transfers. Additionally, examiners may assess a firm's fund transfer request authentication procedures.

2. Vendor management: Examiners may assess a firm's vendor selection and management practices (including the level of due diligence conducted during vendor selection, monitoring and oversight of vendors, and contract terms) in the context of the firm's ongoing risk assessment process.
3. Training: Examiners may assess whether cybersecurity training is tailored to specific job functions, including cyber incident response procedures, and is designed to encourage responsible employee and vendor behavior.
4. Incident response: Examiners may assess whether a firm has a framework (including policies; system vulnerability assessments; and assessing critical data, assets and services) to address possible future events.

The Risk Alert emphasizes that these factors are not exhaustive and do not create a potential safe harbor from liability. The OCIE may expand the focus of examinations as necessary.

Implications

This Risk Alert exemplifies how the SEC continues to examine both how its existing authority can be used in the cybersecurity area and how that authority might be broadened and strengthened.[5] It also emphasizes that technical controls are only part of the story. Organizational and administrative efforts, including governance, training and vendor oversight, are also crucial.

---

[1] The 2015 Risk Alert.

[2] The SEC's Division of Investment Management also issued cybersecurity guidance in April 2015.

[3] The NIST Cybersecurity Framework.

[4] The FINRA report; The SEC report; WilmerHale's previous alert on the SEC and FINRA reports.

[5] The SEC and FINRA Increase Scrutiny of Regulated Firms' Cybersecurity; The SEC's Two Primary Theories in Cybersecurity Enforcement Actions

Authors

Yoon-Young Lee

SENIOR COUNSEL

yoon-young.lee@wilmerhale.com

+1 202 663 6720