Cybersecurity 2: Insights from OCIE's Recent Round of Cybersecurity Exams

By Benjamin Kozinn Esq., Scott H. Moss Esq., and Preeti Krishnan Esq.

On August 7, 2017, the SEC's Office of Compliance Inspections and Examinations ("OCIE") issued a risk alert providing a summary of observations from its recent exams conducted pursuant to the Cybersecurity Examination Initiative announced on September 15, 2015.[1] The SEC reviewed policies and procedures of 75 broker-dealers, investment advisers and investment companies.

Background

As SEC Chairman Jay Clayton noted in his first policy speech on July 12, 2017, cybersecurity is and will continue to be a significant area of focus for the SEC in 2017.[2] OCIE's most recent round of cybersecurity exams ("Cybersecurity 2") built upon OCIE's 2014 cybersecurity initiative ("Cybersecurity 1"). In this round of exams, OCIE noted improvement in cybersecurity preparedness and simultaneously identified areas where compliance and internal controls could be improved or refined.

Areas of Improvement

OCIE's alert noted certain deficiencies with the maintenance and implementation of examinees' cybersecurity policies, procedures and protocols. SEC-registered broker-dealers, investment advisers and investment companies should evaluate the following areas of their cybersecurity programs to determine if they meet the implicit standards highlighted by the alert:

- *Tailored Policies and Procedures.* Similar to the tailored requirements of a firm's broader compliance manual, cybersecurity policies should reflect the specific attributes of the organization (e.g., investment strategy, number of personnel, number of offices, information technology requirements, etc.) – they should not be generic or vague. Additionally, a firm must enact procedures to facilitate implementation of its policies.
- *Adherence to Policies and Procedures.* Strict adherence to the written cybersecurity policies and procedures of a firm is critical. For example, if an adviser's policies require an "ongoing" review of security protocols, OCIE's alert indicates that an annual (or less frequent) review is inadequate. Additionally, firms should enforce mandatory cybersecurity training requirements and take action against an employee for noncompliance – simply having a policy that mandates training is not sufficient.
- *Safeguarding Information.* Employees should receive specific, well-articulated procedures regarding safeguarding information – policies should not be vague guidance on a limited set of issues.
- *Fund Transfers.* Policies that authorize remote customer access and investor fund transfers should be clear and distinct so that employees have an unambiguous understanding of permissible activity.
- *Remediation.* Firms must ensure that they quickly remediate any high-risk areas identified in penetration testing – testing alone is not sufficient.
- *Incident Response.* Firms should maintain plans for data-breach incidents, including processes for notifying customers of material data breaches.

Improvements and "Robust" Practices

OCIE highlighted the following elements included in cybersecurity policies and procedures of firms that OCIE believed had "implemented robust controls":

- *Inventory and Risk Classifications.* Maintaining a comprehensive inventory of data, information and vendors along with detailed risk, vulnerability, data and business risk rating.
- *Testing and Monitoring.* Establishing specific, detailed penetration tests, security monitoring and system auditing frameworks.
- *Vulnerability Assessments.* Creating detailed schedules and processes for testing data integrity and system vulnerability,

[1] The risk alert is available at https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.

[2] Chairman Jay Clayton's speech is available at https://www.sec.gov/news/speech/remarks-economic-club-new-york.

including vulnerability scans of core information technology infrastructure (and taking action on any issues identified).
- *Security Patches.* Establishing policies that include initially beta testing security patches with a small number of users and servers and analyzing and solving any issues thereafter.
- *Access Controls.* Establishing and maintaining access controls such as employee "acceptable use" policies, enforcing encryption and other restrictions on mobile access to servers, requiring third-party logs with respect to firm server access, and requiring prompt termination of access for persons no longer with the firm.
- *Employee Training.* Mandating employee training of cybersecurity risks and ensuring such training is completed by all employees in a timely manner.
- *Senior Management Involvement.* Ensuring that all policies and procedures are reviewed and approved by senior management.

Consistent Practices

In contrast to Cybersecurity 1, OCIE's alert highlighted the following cybersecurity practices that have become more consistent in examinees:

- Nearly all firms conducted periodic risk assessments.
- Most firms conducted penetration tests.
- Nearly all firms established system maintenance processes.
- All firms maintained policies, procedures and standards for detecting and monitoring data loss.
- Nearly all firms maintained policies and procedures regarding cyber-related business continuity planning, Regulation S-P and Regulation S-ID.
- Nearly all firms developed response plans to access issues.
- Nearly all firms maintained cybersecurity-related organization charts.
- Nearly all firms conducted or required vendor risk assessments and reports.
- The vast majority of firms verified the authenticity of customers and shareholders attempting to transfer funds.

Observations and Recommendations

As noted, OCIE's 2017 priorities include cybersecurity as a continued area of focus for the SEC. We believe, based on the SEC's past practices in exams, that the findings set forth in OCIE's alert will establish a benchmark against which future examinees will be measured. It is likely that the practices of firms that were mentioned as having "robust controls" will become the expected standards for registrants. Firms should evaluate their cybersecurity policies and procedures in light of the key findings and implicit recommendations outlined in OCIE's risk alert. Most importantly, OCIE's alert reinforces the principles that advisers must continue to review their policies to ensure that they are appropriately tailored to their firms' unique attributes and that adherence to such written policies and procedures will continue to be a focus of SEC examiners. For example, firms should consider shifting their review guideline timelines from generalized time frames such as "ongoing" or "from time to time" in favor of more definitive timelines in policies reflected on a compliance calendar. Lastly, in evaluating the adequacy and appropriateness of their cybersecurity policies, firms need to analyze how such policies interact with, among other policies, a firm's business continuity, disaster recovery, and books and records policies. Cybersecurity policies do not, and should not, sit on an island. In today's world, cybersecurity policies need to be an integral part of a firm's overall compliance program.

Contacts

Please contact any of the attorneys listed, or any other member of Lowenstein Sandler's Investment Management Group, if you have any questions regarding OCIE's alert or steps that your firm should consider in light of OCIE's findings.

Benjamin Kozinn, Esq.
Partner
T 212.419.5870 | bkozinn@lowenstein.com

Scott H. Moss, Esq.
Partner
T 646.414.6874 | smoss@lowenstein.com

Preeti Krishnan Esq.
Associate
T 646.414.6910 | pkrishnan@lowenstein.com