The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 30830

August 11, 2017

OCIE Publishes Risk Alert on Observations From Its Second Cybersecurity Review of 75 Registrants

[30830]

August 11, 2017 TO: ICI Members
Investment Company Directors
Chief Compliance Officer Committee
Chief Information Security Officer Advisory Committee
Compliance Advisory Committee
Internal Audit Committee
Technology Committee SUBJECTS: Cybersecurity RE: OCIE Publishes Risk Alert on Observations From Its Second Cybersecurity Review of 75 Registrants

Earlier this week, the SEC's National Exam Program published a Risk Alert summarizing OCIE's observations from the second round of cybersecurity reviews it conducted.[1] These reviews were conducted of 75 firms (broker-dealers, investments advisers, and mutual funds) between September 2015 and June 2016 and involved the review of registrants' activities between October 1, 2014 and September 30, 2015. Unlike OCIE's first round of cyber reviews,[2] this round focused on validation and testing of registrants' procedures and controls surrounding their cybersecurity preparedness.[3] Overall, OCIE "observed increased cybersecurity preparedness" since its 2014 review.[4]

The Risk Alert summarizes OCIE's observation under three headings: Summary of Examination Observations; Issues Observed; and Elements of Robust Policies and Procedures. The staff's observations in each of these areas is briefly summarized below.

Summary of Examination Observations[5]

The review found that "all broker-dealers, all funds, and nearly all advisers examined maintained cybersecurity-related written policies and procedures addressing the protection of customer/shareholder records and information."[6] Other observations included the following:

- **Periodic Risk Assessments:** Nearly all broker-dealers and the "vast majority" of funds and advisers conducted periodic risk assessments of critical systems to identify cyber threats, vulnerabilities, and the potential business consequences of an attack.
- **Penetration Testing and Vulnerability Scans:** Nearly all broker-dealers "and

almost half of the advisers and funds" conducted penetration testing and vulnerability scans on critical systems though "a number of firms" did not fully remediate high-risk observations discovered during these tests and scans.

- **Breach Monitoring:** All firms used some form of system, utility, or tools to prevent, detect, and monitor data loss relating to personally identifiable information.
- **Patch Installation:** All broker-dealers and nearly all advisers and funds had processes to ensure regular system maintenance, including installing patches. The staff observed, however, that a few firms had failed to install "a significant number" of patches to critical systems.
- **Breach Response:** While "the vast majority of firms" had plans addressing denial of service incidents and unauthorized intrusions and "the vast majority of broker-dealers" maintained plans for data breach incidents, including notifying customers of material events, "less than two-thirds of the advisers and funds appeared to maintain such plans."
- **Organizational Charts Relating to Cyber:** All broker-dealers "and a large majority of advisers and funds" maintained organizational charts or information that identified and described cybersecurity roles and responsibilities for the firms' workforce.
- **Customer Verification for Transfers:** For those firms that permitted the transfer of account assets to third-party accounts, all funds and advisers maintained policies, procedures, and standards related to verifying the authenticity of a customer/shareholder who was requesting the transfer.[7]
- **Vendor Risk Assessments:** "Almost all firms" either conducted vendor risk assessments or required vendors to provide them with risk management and performance reports and securities reviews or certification reports. The Risk Alert notes that, in addition to conducting vendor reviews at the outset of a relationship, "over half of the firms also required updating . . . on at least an annual basis."

Issues Observed[8]

The issues listed in this section of the Risk Alert are those that the staff found in the "vast majority" of firms they visited. These are as follows:

- **Concerns with Registrants' Policies and Procedures:** While registrants maintained written policies and procedures relating to cyber-related issues, "a majority" of the firms' policies "appeared to have issues." These included policies that were not sufficiently tailored to the firm; policies that were not enforced; or policies that did not reflect the firm's actual practices.
- **Concerns Related to Reg. S-P Compliance:** The staff observed firms "that did not appear to adequately conduct system maintenance" (*e.g.,* installing patches) "and other operational safeguards to protect customer records and information." Examples of this included using outdated systems that were no longer supported by security patches and not remediating in a timely fashion "high-risk findings" from penetration tests or vulnerability scans.

Elements of Robust Policies and Procedures[9]

The Risk Alert also includes examples of elements the staff observed in firms that, in the staff's view, "had implemented robust controls." These included the following:

- **Maintaining Complete and Current Inventories:** The staff observed firms that maintained complete and current inventories of data, information, and vendors and included a classification of risks, vulnerabilities, data, business consequences, and information regarding each of its vendor and service providers "if applicable."
- **Including in the Firm's Policies and Procedures Detailed Cybersecurity-**

Related Instructions: Examples of such instructions included provisions relating to: reviewing the effectiveness of security solutions following penetration testing; detailed instructions regarding appropriate testing and methodologies when conducting security monitoring and system audits; tracking and keeping current access rights; and reporting protocols to use when an event occurs.

- **Maintaining Prescriptive Schedules and Processes for Testing Data Integrity and Vulnerabilities:** Examples included: prioritizing action items from vulnerability scans of key systems and patch management policies that (1) involved beta testing with a limited group of users prior to firm-wide deployment and (2) an analysis of the effectiveness of the patch.
- **Establishing and Enforcing Access Controls:** Effective practices in this space included implementing detailed policies "that specified employees' obligations when using the firm's network and equipment;" requiring and enforcing restrictions (*e.g.,* passwords, encryption) on mobile devices connected to the firm's systems; requiring "third-party vendors to periodically provide logs of their activity on the firms' networks;" and requiring immediate termination of terminated employees' access to systems.
- **Mandatory Employee Training:** Effective training involved training all employees when hired and periodically thereafter, with monitoring to verify employees completed such training.
- **Engaged Senior Management:** The staff observed the engagement of senior managements in vetting and approving the firm's policies and procedures.

The Risk Alert notes that, during 2017, cybersecurity reviews will continue to be a priority for OCIE and OCIE plans to examine registrants "for cybersecurity compliance procedures and controls, including testing the implementation of those procedures and controls at firms".

Tamara K. Salmon
Associate General Counsel

endnotes

[1] *See Observations From Cybersecurity Examinations,* SEC National Exam Program Risk Alert (Vol. VI, Issue 5; August 7, 2017) ("Risk Alert"), which is available at: https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.

[2] OCIE's first round of cyber reviews involved 57 broker-dealers and 49 registered investment advisers. It involved a review of registrants' practices in 2013 through April 2014 and focused on their policies and procedures. In February 2015, OCIE published a Risk Alert summarizing its observations from this review. *See* https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

[3] As part of this review, and to better understand how registrants managed their cybersecurity preparedness, the review considered registrants' (1) governance and risk assessments; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response.

[4] The two reviews involved different registrants.

[5] These observations can be found on pp. 2-3 of the Risk Alert.

[6] Risk Alert at p. 2. The Risk Alert additionally notes that in their first cyber review, “comparatively fewer broker-dealers and advisers had adopted [such] policies and procedures.”

[7] According to the Risk Alert, the “vast majority” of broker-dealers and “nearly two-thirds of the advisers and funds” permitted such transfers. The Risk Alert found that “some of the broker-dealers” had informal practices for verifying customer’s identities.

[8] These observations can be found on pp. 3-4 of the Risk Alert.

[9] These observations can be found on pp. 4-5 of the Risk Alert.
