ROPES & GRAY ALERT

Asset Management ▪ Privacy & Data Security

September 18, 2015

SEC's OCIE Risk Alert Announces New Cybersecurity Exam Initiative – Focus Includes Conducting Tests of Efficacy of Firm's Procedures and Controls

Following up on last year's cybersecurity sweep exam, the SEC's Office of Compliance Inspections and Examinations ("OCIE") issued a new Risk Alert on September 15, 2015, announcing a second round of cybersecurity exams. In addition to gathering information about industry practices, OCIE announced that it intends to test individual firms' implementation of cybersecurity procedures and controls. OCIE also included with the Risk Alert a comprehensive five-page sample inspection document request letter ("Exam Letter"). While the Risk Alert states the Exam Letter is to assist firms' assessments of their individual cybersecurity preparedness, it also provides a guide to what OCIE likely will consider to be components of a reasonable cybersecurity program. Therefore, advisers and firms would be well-advised to review and assess their own programs in light of OCIE's Exam Letter.

The Risk Alert emphasized that OCIE will focus on six core areas in the second round of exams:

1. Governance and Risk Assessment. OCIE will look for the existence of cybersecurity policies, procedures and processes, and whether those are reviewed on a regular basis. Importantly, the Risk Alert also notes OCIE will be examining the level of communication to, and involvement of, senior management and boards regarding cybersecurity issues.
2. Access Rights and Controls. The Risk Alert notes the importance of access controls to preventing data breaches, including multi-factor authentication (e.g., use of RSA tokens to access firm systems in addition to user names and passwords) and updating access rights with personnel or system changes. Review of a firm's access controls may include examination of network segmentation, remote access controls, and firm protocols to address reports of customer login problems.
3. Data Loss Prevention. The Risk Alert highlights the importance of robust patch management and system configuration controls as part of a cybersecurity program, and any review likely will include the efficacy of a firm's implementation of any such controls. Of note, the Risk Alert also states that OCIE may review whether and how a firm monitors its own network traffic, including monitoring for unauthorized data transfers and for the volume of content transferred outside of the firm by its employees or to third parties.
4. Vendor Management. The Risk Alert states that reviews may include a focus on a firm's practices and controls concerning vendor management, including vendor selection, due diligence, monitoring and contractual terms.
5. Training. The Risk Alert places an emphasis on firms performing proper training of employees and vendors. OCIE intends to review how training is tailored to specific job functions, and how training is designed to encourage responsible employee and vendor behavior. OCIE also intends to examine how a firm's procedures for responding to cyber-incidents (under an incident response plan) are integrated into regular training of employees and vendor personnel.
6. Incident Response. OCIE also may assess whether a firm has established policies, assigned roles, identified vulnerabilities, and developed plans to address possible future cyber-events.

The Exam Letter provides more information regarding the extent to which an inspection may dig into the details of a firm's information security program with respect to the six core areas. Firms may find the Exam Letter's list of items that OCIE may ask to review to be of particular interest. These items include:

- evidence of board minutes and briefings regarding cybersecurity issues;
- descriptions of the kinds of periodic assessments of cybersecurity that a firm performs;
- information about a firm's ability to monitor its systems and log abnormal events and testing of red flag rule procedures;
- a firm's written policies and procedures related to enterprise data loss prevention, including information concerning information ownership and how the firm documents or evidences personally identifiable information;
- evidence of due diligence with regard to vendor selection and monitoring by the firm;
- descriptions of the training provided by a firm to its employees about information security and risks; and
- information regarding a firm's processes for testing its incident response plans.

The subject matter detail in the questionnaire follows on some of the very specific cybersecurity guidance the SEC provided in its April 2015 Division of Investment Management Guidance Update titled Cybersecurity Guidance (described here). Together, they suggest increased expectations by the SEC on what firms should be doing as part of a reasonable cybersecurity program. As OCIE's February 2015 summary of its findings from its first cybersecurity sweep exam shows, some regulated entities, particularly asset management firms, may currently fall short of those expectations.

For further information about how this update may impact your interests, please contact your regular Ropes & Gray contact or a member of Ropes & Gray's leading privacy and data security team.