BRACEWELL

INSIGHTS

SEC: 2015 Examination Priorities – Cybersecurity Compliance and Controls

September 17, 2015

Registered broker-dealers and investment advisers received a stern warning to strengthen their cybersecurity programs or face further regulatory scrutiny. On September 15, 2015, the SEC announced a plan to sharpen its focus on securities firms' cybersecurity programs through the National Exam Program. Specifically, the SEC issued a Risk Alert, authored by the Office of Compliance Inspections and Examinations (OCIE), revealing a second round of cybersecurity examinations of registered broker-dealers and investment advisers. The Risk Alert provides helpful guidance for firms that need to develop a cybersecurity program or improve on an existing program. This increase in testing is a marked change from the first round of examinations in 2014, which consisted mainly of oral interview and document reviews.

The Risk Alert provides that the upcoming examinations will center on the following areas:

1. Governance and Risk Assessment: The SEC may assess the firm's cybersecurity policies and risk assessment policies. Further, the Risk Alert provides that the SEC may look at the level of communication between executives and board members regarding cybersecurity. This highlights a growing focus on board-level involvement in cyber and data protection issues that cannot be ignored; data protection is no longer simply an IT function.

2. Access Rights and Controls: The Risk Alert notes that firms may be at a particular risk in this area for failing to implement basic controls. The SEC may assess policies and procedures regarding data usage and permissions; that is, which employees can see what data, when, and from where. Further, this area of inquiry will include evaluating the required level of sophistication for passwords and whether there are multiple layers of protection, such as two-step verification, for remote entry to company servers.

3. Data Loss Prevention: The SEC may assess the methods used to monitor the data transferred outside the firm and how firms assess customer requests for fund transfers.

4. Vendor Management: As some of the largest data breaches have occurred via third-party entry, the SEC may evaluate the firm's policies with respect to vendor data protection. There can be significant ramifications if the firm has adequate data protection policies for internal processes but allows its vendors to get by with a lower standard.

5. Training: Far too many data breaches occur because of employee error. Highlighting this fact, the Risk Alert suggests that the SEC may evaluate the level of training employees receive on data protection and how often that training is updated and repeated. The Risk

Alert suggests that properly trained employees can act as a "first line of defense" against the loss of valuable data.

6. Incident Response: This area involves a firm's crisis response plan. The SEC may evaluate whether the firm has identified its information that is most vulnerable to attack; what it purports to do about it; how it plans to react if the firm's prized information is taken; and what employees have been pre-assigned roles for reacting efficiently and effectively to such an intrusion. A crisis response plan is essential for a firm hoping to make it through a cyber breach with its reputation and business intact.

The SEC warned that the list is not exhaustive and may be supplemented at any time. To further help with compliance, the OCIE attached a sample examination request for information and documents that it hopes will "encourage registered broker-dealers and investment advisers to reflect upon their own practices, policies, and procedures with respect to cybersecurity." Take heed broker-dealers and investment advisers, the SEC's areas of examination focus and document requests are a roadmap to the regulator's priorities and expectations for your firm's cybersecurity program. When the OCIE examiners show up at your door with little forewarning, it will be too late to implement a cybersecurity program or improve a lax preexisting one.

The Risk Alert in its entirety may be accessed ***here.***