Blogs
August 18, 2017
SEC Offers More Guidance on Cybersecurity Best Practices and Pitfalls - Part 2 of 2

This post continues our discussion of the Risk Alert released on August 7, 2017, by the SEC's Office of Compliance Inspections and Examinations ("OCIE") regarding conclusions drawn from its yearlong review of the cybersecurity practices of 75 asset management firms and funds. The sweep, deemed OCIE's Cybersecurity 2 Initiative, covered broker-dealer, investment adviser, and investment company practices during the period from October 2014 through September 2015.

Elements of Effective Policies and Procedures

The Risk Alert identifies the elements of policies and procedures that the OCIE staff believes should be part of a "robust" set of cybersecurity controls. In addition to the major elements of a healthy cybersecurity program discussed in part 1 of this blog, the OCIE staff in the Risk Alert urges asset management firms to also consider the following critical elements.

Maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities.

- Firms with cybersecurity policies and procedures that the OCIE staff found to be strong conduct vulnerability scans of core IT infrastructure to aid in identifying potential key system vulnerabilities, and maintain logs of prioritized action items for any identified concerns.
- Policies and procedures that the OCIE staff support call for appropriate patch management policies that include (i) beta testing of patches with a small number of users and servers before firm-wide deployment, (ii) an analysis of the problem each patch is intended to fix, (iii) the potential risks in applying the patch, and (iv) the method to be used in applying the patch.

Established and enforced controls to access data and systems.

- Firms the OCIE staff viewed favorably implement detailed "acceptable use" policies that specify employees' obligations when using firm networks and equipment.
- Robust programs require and enforce restrictions and controls for mobile devices connected to firm systems, such as password protection and the use of encrypted communication.
- Firms with strong cybersecurity policies and procedures require third-party vendors to periodically turn over logs of their activity on the firm's networks and require immediate termination of access for terminated employees, and very prompt (typically, same day) termination of access for employees leaving voluntarily.

Mandatory employee training.

The OCIE staff is supportive of firms that make information security training mandatory for all employees, both upon initial hire and then periodically, and of firms that institute policies and procedures to ensure that employees complete the mandatory training.

Engaged senior management.

Healthy cybersecurity programs identified by the OCIE staff require their policies and procedures to be vetted and approved by senior management.

Key Takeaways

Cybersecurity remains a paramount concern of the SEC, appearing on OCIE's 2017 Examination Priorities list. This most recent Risk Alert comes as well-publicized cyber attacks have demonstrated that even the strongest IT system can be vulnerable to cybersecurity issues. It also comes as the cybersecurity consulting and insurance industries continue to expand, with greater capacity than ever before. Asset management firms and fund boards should take advantage of the guidance offered by the OCIE staff in the Risk Alert to reassess their cybersecurity policies and procedures in this environment. Simply having such policies and procedures in place, the Risk Alert makes clear, is not enough, and OCIE plans to "continue to examine for cybersecurity compliance procedures and controls, including testing the implementation of those procedures and controls at firms." To prepare for such examination, firms and fund board policies should work to make sure that their cybersecurity programs include actionable incident response plans that are executable by employees. They should seek to ensure that cybersecurity policies and procedures are reasonably tailored to the firm's or fund's actual operations such that they are followed in actual practice. This could be achieved through an independent assessment or regular reporting from appropriate IT personnel. The OCIE staff seems to view cybersecurity incidents not as matters of if, but when, and suggests that when an attack does occur, everyone, from the chair of the board to the entry-level employee, should be able to rely on a set of well?developed, well-tested procedures on which they have been trained. The guidance offered in the Risk Alert should help in establishing such a robust cybersecurity program.

Explore more in

Investment Management