Akin®

SEC OCIE Sharpens Focus on Cybersecurity

Sep 21, 2015

Reading Time : **2 min**

By: Natasha G. Kohne, Jo-Ellyn Sakowitz Klein, Prakash H. Mehta, Eliot D. Raffkind, David S. Turetsky, Visiting Professor, College of Emergency Preparedness, Homeland Security, and Cybersecurity at the University of Albany

This Risk Alert builds upon a report issued by the OCIE in February 2015, after it conducted its first round of cybersecurity examinations beginning in April 2014. That report highlighted some of the cybersecurity risk areas for investment advisers and broker-dealers. According to the latest Risk Alert, the OCIE elected to launch a second initiative in order to promote better compliance practices and further the SEC's understanding of cybersecurity preparedness.

The Risk Alert identifies specific areas of focus for the second round of cybersecurity examinations:

- Governance and Risk Assessment – Are firms periodically evaluating security risks and tailoring their controls to their business? Examiners may review the communications of senior management and the board of directors, including, but not limited to, board minutes and briefing materials, to assess their involvement. Examiners may also seek information regarding a firm's chief information security officer, and other employees responsible for cybersecurity matters.
- Access Rights and Controls – Are firms updating access rights based on personnel or system changes? Examiners may review the controls associated with remote access, customer logins and passwords, such as use of multifactor authentication.
- Data Loss Prevention – Do firms have robust controls in the areas of patch management and system reconfiguration? Examiners may assess how firms monitor

content transferred to and from the firm and the authenticity of customer requests to transfer funds.

- Vendor Management – Do firms have practices and controls in place related to the risk of hacking of third-party vendor platforms? Examiners may assess how vendors are selected and monitored.
- Training – Do firms have appropriate training programs in place? Examiners may assess how training is tailored to specific job functions, designed to encourage responsible employee behavior and updated to reflect cyber incidents.
- Incident Response – Do firms have established policies, assigned roles and developed plans to respond to cybersecurity attacks? Examiners may review information regarding breaches, losses and remediation, tests or exercises of the incident response plan and cyber insurance.

Key Takeaways

Firms should begin preparing now for this second round of examinations. The OCIE has attached to the Risk Alert a sample request for information and documents; firms can expect the OCIE to issue such requests in short order. Firms should use this sample request to assess their own policies and procedures in advance of having to respond to the OCIE.

Categories

Cybersecurity, Privacy & Data Protection | Compliance

other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.