OCIE's 2015 Cybersecurity Examination Initiative

Written by Catherine M. Anderson

September 18, 2015

Second Round of Cybersecurity Examinations to Begin

On September 15, 2015, the Office of Compliance Inspections and Examinations (OCIE) of the Securities and Exchange Commission (SEC) issued a Risk Alert announcing a second round of examinations of registered investment advisers and broker-dealers under its cybersecurity examination initiative. The Risk Alert's purpose is to provide additional information on the areas of focus for the OCIE's examinations, which will involve more testing to assess implementation of firm procedures and controls.

Registered investment advisers should review their current cybersecurity practices, policies and procedures to ensure that they have addressed the matters referred to in the sample request for information which is included as an Appendix to the Risk Alert and consult with their IT service providers, as appropriate. They will likely be asked to provide this information on an SEC examination.

In summary, the OCIE is planning to assess the following key areas:

- **Governance and Risk Assessment**: protection of client information procedures, board minutes and briefing materials regarding cybersecurity, Chief Information Security Officer position, organizational structure, periodic testing and risk assessment for cybersecurity-related matters.
- **Access Rights and Controls**: how firms control onsite and offsite access to various systems and data, including the management of user credentials, authentication, and authorization methods.
- **Data Loss Prevention**: how firms monitor outbound communication and data transferred by employees or third parties.
- **Vendor Management**: how firms conduct diligence and monitor downstream compliance controls of third-party vendors, and contingency planning.
- **Training**: how firms train employees and third-party vendors on data security and data breach prevention measures.
- **Incident Response**: whether firms have established proper protocols to prevent and/or respond to cybersecurity attacks, including developing plans to assess system vulnerabilities and to address possible future incident and cybersecurity insurance.

For additional information on the cybersecurity focus by the SEC see our earlier Foley Adviser updates, which can be found here: **SEC Issues Risk Alert on Cybersecurity Initiative for Investment Advisers** and **SEC Office of Compliance Inspections and Examinations Releases Cybersecurity Examination Sweep Summary of Investment Advisers and Broker-Dealers**.

RELATED INDUSTRIES

- Investment Advisers & Private Funds
- Professional Services

RELATED PRACTICES

- Business Counseling