SEC Office of Compliance Inspections and Examinations Releases Cybersecurity Examination Sweep Summary of Investment Advisers and Broker-Dealers

Written by Catherine M. Anderson, Kate Leonard

February 5, 2015

On February 3, 2015, the Office of Compliance Inspections and Examinations (OCIE) released the findings of its Cybersecurity Examination Sweep, which sought to evaluate the breadth of cybersecurity policies implemented by investment advisers (as well as by broker-dealers). For more details on the sweep, see our previous Foley Adviser update: SEC Issues Risk Alert on Cybersecurity Initiative for Investment Advisers.

The released report examines the varying degrees of preparedness of firms, steps taken to combat cybersecurity threats, the incidence of such threats, and how firms responded to them. Clients are urged to review their cybersecurity practices against the Cybersecurity Examination Sweep report and to take action if there are gaps in their current practices as compared to the industry practices noted.

Key findings of the report include:

- The vast majority of investment advisers (89%) have adopted written information cybersecurity policies. A majority of the investment advisers (57%) conduct periodic audits to ensure compliance with the policies. Few of these policies (13%), however, address whether and to what extent they are responsible for client losses associated with cybersecurity breaches, and even fewer (9%) offer security guarantees to clients as a result of such a breach.
- Many firms are utilizing external standards and other resources to model their information security architecture and processes, such as those published by the National Institute of Standards and Technology, the International Organization for Standardization, and the Federal Financial Institutions Examination Council.
- The vast majority of investment adviser firms conduct periodic risk assessments on a firm-wide basis to identify cybersecurity threats, vulnerabilities, and potential business consequences, as well as inventory, map, and/or catalogue their technology resources. However, fewer (32%) demand the same cybersecurity assessments of their vendors, and very few (24%) incorporate cybersecurity risk policies into vendor contracts.
- 74% of investment adviser firms have experienced a cybersecurity attack directly or through one or more of their vendors, the majority of which took the form of malware and fraudulent e-mails. Significantly, few advisers report fraudulent e-mails to the Financial Crimes Enforcement Network (FinCEN) or other regulatory agencies or law enforcement.
- 91% of investment adviser firms use some form of encryption.
- The designation of a Chief Information Security Officer ("CISO") varied, with fewer than one-third of investment advisers designating a CISO. Rather, advisers often direct their Chief Technology Officer to take on the responsibilities typically performed by a CISO, or they assign another senior officer (e.g., the Chief Compliance Officer, Chief Executive Officer, or Chief Operating Officer) to liaise with a third-party consultant who is responsible for cybersecurity oversight.
- Use of cybersecurity insurance revealed varying findings among the examined firms. Comparatively few (21%) carry cybersecurity insurance, and those that do hardly ever file claims.

The full text of the Cybersecurity Examination Sweep is available here. Cybersecurity continues to be a focal point of the OCIE, as emphasized in their 2015 Examination Priorities.

In addition to these findings, the SEC's Office of Investor Education and Advocacy (OIEA) issued an Investor Bulletin that provides core

tips to help investors safeguard their online investment accounts. The full text of the Investor Bulletin is available here.

RELATED INDUSTRIES

- Investment Advisers & Private Funds
- Professional Services

RELATED PRACTICES

- Business Counseling
