SEC Issues Cybersecurity Guidance Update for Investment Advisers

Written by Catherine M. Anderson, Robert G. Sawyer

April 29, 2015

On April 28, 2015, the SEC's Division of Investment Management (the "Division") issued a Guidance Update regarding the SEC's initiative to assess cybersecurity preparedness and threats in the securities industry, further highlighting this as an important area of focus for the SEC in its compliance initiatives.

The full text of the Guidance Update is **available here**. In summary, the Guidance Update notes the Division staff's view that funds and investment advisers may wish to consider the following in order to address cybersecurity risk in their organizations:

a. **Periodic cybersecurity assessments**, including evaluating the information the firm has in its control, the cybersecurity risks (vulnerabilities and possible impact from systems becoming compromised), current controls and their effectiveness.

b. **Creation of a strategy for prevention, detection and response to threats**, including access controls, data encryption, physical and technological safeguards on portability of data, backup and retrieval solutions and an incident response plan (and routine testing of the foregoing).

c. **Implementation of strategy** by means of written policies and procedures and training to provide employees (and potentially investors and clients) with guidance on potential threats and means to prevent, detect and respond to them, and to monitor compliance.

Further, the Division reminds investment advisers that they could mitigate exposure to any compliance risk associated with cyber threats through compliance policies and procedures that are reasonably designed to prevent violations of already existing federal securities laws (17 CFR 270.38a-1; 17 CFR 275.206(4)-7(a); see also Release No. 26299 (Dec. 17, 2003)). For example, the compliance program of an investment adviser could address cybersecurity risk as it relates to identity theft and data protection (see Identity Theft Red Flag Rules and Regulation S-P), fraud (Release No. 23958 (Aug. 24, 1999)) and business continuity, as well as other disruptions in service that could affect, for instance, a fund's ability to process shareholder transactions.

Investment advisers are encouraged to monitor for ongoing and new cyber threats by gathering information from outside resources, such as vendors, third-party contractors specializing in cybersecurity and technical standards, and topic-specific publications and conferences, as well as participating in the Financial Services—Information Sharing and Analysis Center (FS-ISAC).

SEC-registered investment advisers should review the Guidance Update, consider whether any changes need to be made to their current cybersecurity policies and procedures and make sure that their compliance program is tailored based on the size and nature of their business.

RELATED INDUSTRIES

- Investment Advisers & Private Funds
- Professional Services

RELATED PRACTICES

- Capital Markets
- Business Counseling