SEC Issues Cybersecurity Guidance for Investment Companies and Advisers

Skadden

05/06/15

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Anastasia T. Rockas
New York
212.735.2987
anastasia.rockas@skadden.com

Stuart D. Levi
New York
212.735.2750
stuart.levi@skadden.com

Cyrus Amir-Mokri
New York
212.735.3279
cyrus.amir-mokri@skadden.com

Four Times Square
New York, NY 10036
212.735.3000

skadden.com

In April 2015, the Securities and Exchange Commission (the "SEC") Division of Investment Management issued a guidance update[1] (the "Update") identifying cybersecurity of registered investment companies and registered investment advisers as a critical issue and detailing measures that may be considered to address cybersecurity risks. In many ways, the Update focuses on the same key issues that other regulators have found important for addressing cybersecurity risk, namely risk assessment, effective governance, creating an incident response plan, participating in cyber threat information sharing bodies, assessing the risk posed by third-party vendors and considering cyber insurance.

Background

The Update is part of the SEC's ongoing Cybersecurity Initiative[2] and draws from (1) conversations with fund boards and senior management at investment advisers, (2) the Office of Compliance Inspections and Examinations' review of investment adviser cybersecurity practices[3] and (3) the SEC's Cybersecurity Roundtable that took place in March 2014. The SEC noted that findings from its outreach efforts and cyberattacks on a number of financial services firms make it important that firms review their cybersecurity policies.

Earlier this year, the SEC completed its initial cybersecurity examination sweep of certain registered broker-dealers and registered investment advisers. On February 4, Vincente Martinez, chief of the Office of Market Intelligence in the SEC's Enforcement Division, indicated at the FINRA/SIFMA Cybersecurity Conference that the SEC will conduct additional exams focusing on IT controls of a smaller group of firms.

New Guidance

The Update provides a number of specific measures firms may consider implementing to protect confidential information, including information about fund investors and advisory clients, from a cyberattack The Update recommends that firms (1) conduct periodic assessments to identify cybersecurity threats and areas of vulnerability in order to prioritize and mitigate risk, (2) create a strategy designed to prevent, detect and respond to cybersecurity threats and (3) adopt written policies and procedures to implement the strategy.

Periodic Assessments: The Update recommends that firms conduct periodic assessments in the following areas:

- the nature, sensitivity and location of information that firms collect, process and/or store, and the technology systems used;
- internal and external cybersecurity threats to, and vulnerabilities of, firms' information and technology systems;
- security controls and processes currently in place;

[1] The full text of the Update is available at http://www.sec.gov/investment/im-guidance-2015-02.pdf.

[2] For a more in-depth discussion of the Cybersecurity Initiative, see page 3 of our April 2014 *Privacy & Cybersecurity Update*, available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_April_2014.pdf.

[3] For a more in-depth discussion of the review see page 4 of our February 2015 *Privacy & Cybersecurity Update* available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_February_2015.pdf.

- the impact should the information or technology systems become compromised; and
- the effectiveness of the governance structure for the management of cybersecurity risk.

Strategy Elements: The Update notes that a strategy to address cybersecurity threats could include:

- controlling access to various systems and data via management of user credentials, authentication and authorization methods, firewalls and/or perimeter defenses, tiered access to sensitive information and network resources, network segregation and system hardening;
- data encryption;
- protecting against the loss or exfiltration of sensitive data by restricting the use of removable storage media and deploying software that monitors technology systems for unauthorized intrusions, the loss or exfiltration of sensitive data, or other unusual events;
- data backup and retrieval;
- the development of an incident response plan;
- routing testing of any strategy; and
- participating in information sharing organizations such as the Financial Services – Information Sharing and Analytics Center.

Cybersecurity Policies and Procedures: In order to implement a cybersecurity strategy, the Update recommends that firms adopt written policies and procedures and provide training to employees regarding the strategy. The Update also notes that firms may take a proactive stance towards investors and clients and educate them in ways to reduce cybersecurity threats to their accounts.

Conclusion

The SEC views cybersecurity and a firm's compliance obligations under the federal securities laws as closely connected. Cybersecurity threats can impact a firm's ability to comply with certain federal securities laws and, as a result, firms should examine their ability to respond to cybersecurity threats in that context. For example, policies and procedures that address cybersecurity threats as they relate to other compliance areas — such as identity theft and data protection, fraud, and business continuity and other disruptions — also may improve a firm's ability to meet its compliance obligations in those areas. The Update suggests that firms examine their cybersecurity vulnerability as it relates to the use of service providers and adopt protective measures as necessary.

Recognizing that every firm is different and vulnerabilities are inevitable, the SEC suggests that firms consider their particular circumstances and plan accordingly to develop a response capability to mitigate potential damage to investors, clients and compliance obligations. Cybersecurity will be a continuing area of SEC focus and concern and firms should prepare accordingly.