The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 28940

April 29, 2015

SEC Division of Investment Management Publishes Cybersecurity Guidance

[28940]

April 29, 2015

TO:

COMPLIANCE MEMBERS No. 16-15
CHIEF RISK OFFICER COMMITTEE No. 11-15
INTERNAL AUDIT ADVISORY COMMITTEE No. 6-15
TECHNOLOGY COMMITTEE No. 6-15
CHIEF INFORMATION SECURITY OFFICER ADVISORY COMMITTEE
SMALL FUNDS MEMBERS No. 20-15
OPERATIONS MEMBERS No. 16-15

RE:

SEC DIVISION OF INVESTMENT MANAGEMENT PUBLISHES CYBERSECURITY GUIDANCE

The SEC's Division of Investment Management has published guidance to highlight the importance of cybersecurity and provide guidance to funds and advisers on this topic. [1] The Guidance discusses three measures that funds and advisers "may wish to consider in addressing cybersecurity risks" and recommends that registrants take into account cybersecurity considerations when identifying their compliance obligations under the Federal securities laws. The Guidance's discussion of these issues is briefly summarized below. Importantly, while the Guidance recognizes that it is "not possible for a fund or adviser to anticipate and prevent every cyber attack," in the view of the staff, "[a]ppropriate planning to address cybersecurity and a rapid response capability may, nevertheless, assist funds and advisers in mitigating the impact of any such attack and any related effects on fund investors and advisory clients, as well as complying with the federal securities laws." [2]

Measures Firms May Want to Consider Taking to Address Cybersecurity Concerns

According to the Guidance, funds and advisers may wish to consider taking the following

measures, “to the extent they are relevant,” to address cybersecurity risks:

(1) Conduct a periodic assessment. Such assessment should consider:

- The nature, sensitivity, and location of information the firm collects, possesses, and/or stores, and the technology systems it uses;
- Internal and external cybersecurity threats to and vulnerabilities of the firm’s information and technology systems;
- Security controls and processes currently in place;
- The impact of the information or technology systems becoming compromised; and
- The effectiveness of the governance structure for the management of cybersecurity risk.

The Guidance notes that an effective assessment of these areas would assist the firm in identifying potential cybersecurity threats and vulnerabilities so it could better prioritize and mitigate risks. It also advises funds and advisers that are affiliated with other entities that share common networks to consider whether it may be appropriate to conduct an assessment of the entire corporate network.

(2) Create a strategy that is designed to prevent, detect, and respond to cybersecurity threats. The elements of this strategy might include the following:

- 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; [3]
- Data encryption;
- Protecting against the loss or exfiltration of sensitive data by: restricting the use of removable storage media; deploying software that monitors technology systems for unauthorized intrusions, the loss or exfiltration of sensitive data, or other unusual events; and data backup and retrieval; and
- The development of an incident response plan.

In addition to creating a strategy, firms may want to consider routine testing of it to enhance its effectiveness. Firms may also wish to consider implementing a mechanism to monitor for ongoing and new cyber threats by gathering information from outside resources as well as through participating in the Financial Services – Information Sharing and Analysis Center (FS-ISAC). [4]

(3) Implement the strategy through written policies and procedures and training. Such training should provide guidance to officers and employees concerning applicable threats and measures to prevent, detect, and respond to such threats. Firm should consider monitoring compliance with cybersecurity policies and procedures and they may want to educate investors and clients about how to reduce their exposure to cybersecurity threats concerning their accounts.

The Impact of Cybersecurity on a Fund or Adviser’s Compliance Obligations

The Guidance recommends that funds and advisers identify their respective compliance obligations under the federal securities laws and take these obligations into account when assessing the firm’s ability to prevent, detect, and respond to cyber attacks. [5] It notes

that registrants could mitigate exposure to compliance risks associated with cyber threats "through compliance policies and procedures that are reasonably designed to prevent violations of the federal securities laws." [6] As part of this process, registrants "may wish to consider reviewing their operations and compliance programs to assess whether they have measures in place that are designed to mitigate their exposure to cybersecurity risk." [7] They also may wish to consider assessing whether protective cybersecurity measures are in place at relevant service providers. [8] As registrants consider measures to mitigate their exposure to cybersecurity risks, "they should tailor their compliance programs based on the nature and scope of their business." [9] Footnotes to this portion of the Guidance discuss an adviser's fiduciary duty to its clients to protect such clients from inappropriate behavior by advisory employees and avoid putting clients at risk as a result of an adviser's inability to provide advisory services.

ICI Information Security Resource Center

The Institute's Information Security Resource Center provides reference tools that may be of value to members as they consider the Guidance. The Resource Center is available on the ICI's website at: http://www.ici.org/info_security.

Tamara K. Salmon
Associate General Counsel

endnotes

[1] See IM Guidance Update No. 2015-02: Cybersecurity Guidance, SEC Division of Investment Management (April 2015) ("Guidance"), which is available at: http://www.sec.gov/investment/im-guidance-2015-02.pdf.

[2] Guidance at p. 3.

[3] According to the Guidance, "system hardening" refers "making technology systems less susceptible to unauthorized intrusions by removing all non-essential software programs and services, unnecessary usernames and logins and by ensuring that software is updated continuously." Guidance at fn. 5.

[4] The Institute's Information Security Resource Center, discussed below, includes a list of information sharing resources. See http://www.ici.org/info_security.

[5] Examples cited in the Guidance of potential violations funds and advisers should consider in identifying their compliance obligations include: identity theft, data protection, fraud, business continuity, and service disruptions that impact shareholder transactions such as those that would preclude redeeming shares in compliance with Section 22(e) of the Investment Company Act or investing or managing assets consistent with representations and legal requirements.

[6] Guidance at p. 2.

[7] Id.

[8] According to the Guidance, “service providers may be given limited access to a fund’s technology systems that may inadvertently enable unauthorized access to data held by the fund. Funds, as well as advisers, may wish to consider reviewing their contracts with their service providers to determine whether they sufficiently address technology issues and related responsibilities in the case of a cyber attack. [They] may also wish to consider assessing whether any insurance coverage related to cybersecurity risk is necessary or appropriate.” Guidance at fn. 12.

[9] Guidance at p. 2.
