IM Guidance Update

APRIL 2015 | No. 2015-02

CYBERSECURITY GUIDANCE

The Division has identified the cybersecurity of registered investment companies ("funds") and registered investment advisers ("advisers") as an important issue. Both funds and advisers increasingly use technology to conduct their business activities and need to protect confidential and sensitive information related to these activities from third parties, including information concerning fund investors and advisory clients. This guidance update highlights the importance of the issue and discusses a number of measures that funds and advisers may wish to consider when addressing cybersecurity risks. Because of the rapidly changing nature of cyber threats, the Division will continue to focus on cybersecurity and monitor events in this area.

Cyber attacks on a wide range of financial services firms highlight the need for firms to review their cybersecurity measures. Discussions concerning cybersecurity with fund boards and senior management at advisers during the course of the Division's senior level engagement and monitoring efforts also stressed this need, as did input from the Office of Compliance Inspections and Examinations' review of adviser cybersecurity practices.[1] In addition, the Cybersecurity Roundtable hosted by the Commission last spring highlighted the importance of cybersecurity and the issues and challenges it raises for the financial services sector.[2]

In the staff's view, there are a number of measures that funds and advisers may wish to consider in addressing cybersecurity risk, including the following, to the extent they are relevant:[3]

- Conduct a periodic assessment of: (1) the nature, sensitivity and location of information that the firm collects, processes and/or stores, and the technology systems it uses; (2) internal and external cybersecurity threats to and vulnerabilities of the firm's information and technology systems; (3) security controls and processes currently in place; (4) the impact should the information or technology

systems become compromised; and (5) the effectiveness of the governance structure for the management of cybersecurity risk. An effective assessment would assist in identifying potential cybersecurity threats and vulnerabilities so as to better prioritize and mitigate risk.[4]

- Create a strategy that is designed to prevent, detect and respond to cybersecurity threats. Such a strategy could include: (1) 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;[5] (2) data encryption; (3) 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;[6] (4) data backup and retrieval; and (5) the development of an incident response plan. Routine testing of strategies could also enhance the effectiveness of any strategy.

- Implement the strategy through written policies and procedures and training that provide guidance to officers and employees concerning applicable threats and measures to prevent, detect and respond to such threats, and that monitor compliance with cybersecurity policies and procedures. Firms may also wish to educate investors and clients about how to reduce their exposure to cyber security threats concerning their accounts.

In the staff's view, funds and advisers should identify their respective compliance obligations under the federal securities laws and take into account these obligations when assessing their ability to prevent, detect and respond to cyber attacks. Funds and advisers could also mitigate exposure to any compliance risk associated with cyber threats through compliance policies and procedures that are reasonably designed to prevent violations of the federal securities laws.[7] For example, the compliance program of a fund or an adviser could address cybersecurity risk as it relates to identity theft and data protection,[8] fraud,[9] and business continuity,[10] as well as other disruptions in service that could affect, for instance, a fund's ability to process shareholder transactions.[11] Accordingly, funds and advisers may wish to consider reviewing their operations and compliance programs and assess whether they have measures in place that are designed to mitigate their exposure to cybersecurity risk. Because funds and advisers are varied in their operations, they should tailor their compliance programs based on the nature and scope of their businesses. Additionally, because funds and advisers rely on a number of service providers in carrying out their operations, funds and advisers may also wish to consider assessing whether protective cybersecurity measures are in place at relevant service providers.[12]

The staff believes that funds and advisers will be better prepared if they consider the measures discussed herein based on their particular circumstances when planning to address cybersecurity and a rapid response capability. The staff also recognizes that it is not possible for a fund or adviser to anticipate and prevent every cyber attack. Appropriate planning to address cybersecurity and a rapid response capability may, nevertheless, assist funds and advisers in mitigating the impact of any such attacks and any related effects on fund investors and advisory clients, as well as complying with the federal securities laws.[13]

Endnotes

1 *See OCIE Cybersecurity Examination Sweep Summary*, OCIE, National Exam Program Risk Alert, Vol. IV, Issue 4 (Feb. 3, 2015), *available at* http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf (providing summary observations from the examinations of 57 broker-dealers and 49 advisers conducted under OCIE's Cybersecurity Initiative). *See also OCIE Cybersecurity Initiative*, OCIE, National Exam Program Risk Alert, Vol. IV, Issue 2 (Apr. 15, 2014), *available at* http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.

2 *See generally* Cybersecurity Roundtable, SEC, *available at* http://www.sec.gov/spotlight/cybersecurity-roundtable.shtml.

3 These suggested measures are not intended to be comprehensive and other measures may be better suited depending on the operations of a particular fund or adviser. Each fund or adviser should determine whether these or other measures need to be considered in connection with addressing cybersecurity risks.

4 Funds and advisers that are affiliated with other entities that share common networks should consider whether it may be appropriate to conduct an assessment of the entire corporate network.

5 System hardening refers to 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.

6 Funds and advisers may also wish to consider implementing a mechanism 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). In addition, participating in information sharing organizations, such as FS-ISAC, would enable funds and advisers to share cyber threat information with other members in the financial services sector.

7 17 CFR 270.38a-1; 17 CFR 275.206(4)-7(a). *See also generally Compliance Programs of Investment Companies and Investment Advisers*, Investment Company Act Release No. 26299 (Dec. 17, 2003), *available at* www.sec.gov/rules/final/ia-2204.htm ("Compliance Programs") (requiring not only the adoption and implementation of written policies and procedures, but also an annual review for their adequacy and effectiveness of their implementation); *Questions Advisers Should Ask While Establishing or Reviewing Compliance Programs*, SEC Staff Report (May 2006), *available at* http://www.sec.gov/info/cco/adviser_compliance_questions.htm (last modified Feb. 5, 2009) (asking, among other things, whether an adviser's "electronic information systems, both internal and those supplied by third parties, effectively detect and prevent malicious intrusions from internal and external sources") ("Establishing or Reviewing Compliance Programs").

8 *See, e.g.*, *Identity Theft Red Flag Rules*, Investment Advisers Act Release No. 3582 (Apr. 10, 2013), *available at* www.sec.gov/rules/final/2013/34-69359.pdf; *Privacy of Consumer Financial Information (Regulation S-P)*, Investment Advisers Act Release No. 1883 (June 22, 2000), *available at* http://www.sec.gov/rules/final/34-42974.htm. In formulating or reviewing their compliance programs, firms may also wish to consider, as appropriate, addressing the protection of commercial or market-sensitive information, the disclosure of which could adversely affect customers' interests. *See generally Information for Newly-Registered Investment Advisers*, SEC Staff Information Sheet, *available at* http://www.sec.gov/divisions/investment/advoverview.htm (last modified Nov. 23, 2010); Establishing or Reviewing Compliance Programs, *supra* note 7.

9 Fraudulent activity could result from cyber or data breaches from insiders, such as fund or advisory personnel, and funds and advisers may therefore wish to consider taking appropriate precautions concerning information security. *See, e.g.*, 17 CFR 270.17j-1; 17 CFR 275.204A-1. *See also generally Personal Investment Activities of Investment Company Personnel*, Investment Company Act Release No. 23958 (Aug. 24, 1999), *available at* http://www.sec.gov/rules/final/ia-1815.htm (stating that rule 17j-1 "prohibits fraudulent, deceptive or manipulative acts by fund personnel in connection with their personal transactions in securities held or to be acquired by the fund"); *Investment Adviser Codes of Ethics*, Investment Advisers Act Release No. 2256 (July 2, 2004), *available at* http://www.sec.gov/rules/final/ia-2256.htm (stating that rule 204A-1 will benefit advisers "by renewing their attention to their fiduciary and other legal obligations, and by increasing their vigilance against inappropriate behavior by employees").

10 *See* Compliance Programs, *supra* note 7, at n.22 (stating that an "an adviser's fiduciary obligation to its clients includes obligations to its clients from being placed at risk as a result of the adviser's inability to provide advisory services").

11 If a shareholder of an open-end fund initiated a transaction to redeem his or her shares in that fund and an ensuing cyber attack prevented the fund from processing and redeeming the shares, the fund may be in violation of section 22(e) of the Investment Company Act of 1940 ("Investment Company Act") and rule 22c-1 thereunder. Section 22(e) of the Investment Company Act generally prohibits an open-end fund from suspending the right of redemption or postponing the date of payment of redemption proceeds for more than seven days after tender of a security for redemption, whereas rule 22c-1 under the Investment Company Act generally requires an open-end fund selling, redeeming or repurchasing a redeemable security, to do so only at a price based on its net asset value next computed after receipt of a purchase order or redemption request. Cyber attacks could also prevent both funds and advisers from investing or managing assets in a manner consistent with each of their particular representations and/or contractual provisions.

12 For example, 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. Funds and advisers may also wish to consider assessing whether any insurance coverage related to cybersecurity risk is necessary or appropriate.

13 OCIE's Cybersecurity Initiative contained a sample list of requests for information, which included questions that tracked information outlined in the "Framework for Improving Critical Infrastructure Cybersecurity." *See* OCIE Cybersecurity Initiative, *supra* note 1. Funds and advisers may wish to consult this Framework when considering a strategy to mitigate exposure to cyber attacks. *See* National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

IM Guidance Updates are recurring publications that summarize the staff's views regarding various requirements of the federal securities laws. The Division generally issues *IM Guidance Updates* as a result of emerging asset management industry trends, discussions with industry participants, reviews of registrant disclosures, and no-action and interpretive requests.

The statements in this *IM Guidance Update* represent the views of the Division of Investment Management. This guidance is not a rule, regulation or statement of the Securities and Exchange Commission. Further, the Commission has neither approved nor disapproved its content. Future changes in rules, regulations and/or staff no-action and interpretive positions may supersede some or all of the guidance in a particular *IM Guidance Update*.

The Investment Management Division works to:

- protect investors
- promote informed investment decisions and
- facilitate appropriate innovation in investment products and services

through regulating the asset management industry.

If you have any questions about this IM Guidance Update, please contact:
Chief Counsel's Office
Phone: 202.551.6925
Email: IMOCC@sec.gov