US Securities and Exchange Commission Division of Investment Management Issues Guidance on Cybersecurity

In April 2015, staff of the US Securities and Exchange Commission's (SEC's) Division of Investment Management (IM Staff) released a guidance update highlighting a number of measures that registered investment companies and registered investment advisers should consider in addressing cybersecurity risks.[1] The IM Staff issued the guidance update after: it held discussions with advisers' senior management and with investment company boards;[2] the SEC's Office of Compliance, Inspections and Examinations (OCIE) and the Financial Industry Regulatory Authority (FINRA) conducted cybersecurity sweep examinations on advisers and broker-dealers;[3] and the SEC hosted a cybersecurity roundtable.[4] In the guidance update, the IM Staff provided the following non-exclusive[5] set of recommended measures:

- conduct periodic assessments;
- create a cybersecurity strategy; and
- implement the strategy through written policies and procedures, and employee training.

CONDUCT PERIODIC ASSESSMENTS

The IM Staff recommended that investment companies and advisers periodically assess: (i) the nature, sensitivity and location of the information that is collected, processed or stored, and the technology systems used to do so; (ii) internal and external cybersecurity threats to, and vulnerabilities of, the information and systems; (iii) cybersecurity controls that have already been established; (iv) the potential impact of a cybersecurity incident; and (v) the adequacy of their governance framework for the management of cybersecurity risks.

The IM Staff believes that an effective periodic assessment would help identify threats and vulnerabilities, so as to better evaluate and mitigate cybersecurity risks. As part of this assessment, investment companies and advisers that are affiliated with other entities that share common networks should consider conducting an assessment of the entire corporate network. While not specifically mentioned in the guidance update, investment companies and advisers should include third-party service providers with access to their IT systems in their periodic assessments to better understand the potential risks.

CREATE A CYBERSECURITY STRATEGY

The IM Staff recommended that investment companies and advisers develop a strategy for the purpose of preventing, detecting and reacting to cybersecurity threats by:

- controlling access to data and systems;[6]
- using encryption technologies;[7]
- restricting the use of removable storage media and monitoring technology systems for intrusions, data loss or export, or other unusual events;
- implementing data backup and retrieval processes; and
- developing an incident response plan.[8]

The IM Staff believes that routine testing of the strategy could enhance its effectiveness. The IM Staff also recommended that investment companies and advisers stay up-to-date on new and continuing cyber threats by gathering information from outside resources.[9]

IMPLEMENT THE CYBERSECURITY STRATEGY

The IM Staff suggested that investment companies and advisers implement the strategy by developing and instituting written policies and procedures, as well as a training program, that provide guidance to officers and employees concerning relevant cybersecurity threats and the measures used by the investment company or adviser to prevent, detect and respond to them.[10]

The IM Staff recommended that each firm tailor its policies and procedures to its particular circumstances, including the nature and scope of the firm's business, and that the policies and procedures provide for appropriate planning and rapid response to a cyber attack to mitigate damage.

Additionally, in the IM Staff's view, investment companies and advisers should consider their compliance obligations under the federal securities laws when assessing their ability to prevent, detect and respond to cyber attacks. The IM Staff noted that compliance risks associated with cyber threats could be mitigated through the adoption and implementation of polices and procedures that are reasonably designed to prevent violations of the federal securities laws.[11] The IM Staff stated that, for example, investment companies and advisers' compliance programs could address cybersecurity risks as they relate to:

- identity theft and data protection;[12]
- fraud by insiders;[13]
- business continuity plans;[14]
- shareholder transaction processing for investment companies, as required by 1940 Act Section 22(e) and Rule 22c-1 thereunder;[15] and
- ongoing management of assets in a manner consistent with the investment company or adviser's representations to investors or advisory clients and/or their contractual obligations to investors or advisory clients.

The IM Staff also stated that investment companies and advisers should monitor their ongoing compliance with their cybersecurity policies and procedures.

Importantly, the IM Staff acknowledged that it is not possible for an investment company or adviser to anticipate and prevent every cyber attack. However, the IM staff believes that appropriate cybersecurity and response planning could not only help investment companies and advisers mitigate the impact of cyber attacks on the firms as well as investment company investors and advisory clients, but also would assist investment companies and advisers in complying with the federal securities laws.

OTHER SUGGESTIONS

The IM Staff suggested that investment companies and advisers assess whether protective cybersecurity measures are in place at their relevant service providers and review their service provider contracts for appropriate provisions regarding technology issues and cybersecurity and cyber attack responsibilities. The IM Staff's latter suggestion follows after OCIE's observation, during its cybersecurity sweep examination, that few examined advisers incorporated cybersecurity provisions into their contracts with vendors and business partners.[16]

The IM Staff also recommended that investment companies and advisers assess the cybersecurity risk posed by service providers with access to their IT systems. For example, investment companies and advisers should review contracts with vendors from a cybersecurity risk management perspective.[17] While the guidance update does not identify any specific contractual

protections, these would typically include representations and undertakings with respect to the protection of customer information, audit rights to verify information security and immediate notification in the event of actual or suspected unauthorized access to customer information.

In addition, the IM Staff suggested that investment companies and advisers educate their clients about reducing their exposure to cybersecurity risks associated with their accounts.[18]

The IM Staff further suggested that investment companies and advisers consider obtaining cybersecurity insurance. This recommendation follows after OCIE observed that few of the advisers examined during the cybersecurity sweep examination maintained cybersecurity insurance.[19]

For more information about the topics raised in this legal update, please contact any of the following lawyers.

Amy W. Pershkow
+1 202 263 3336
apershkow@mayerbrown.com

Jeffrey P. Taft
+1 202 263 3293
jtaft@mayerbrown.com

Leslie S. Cruz
+1 202 263 3337
lcruz@mayerbrown.com

Andrew Getsinger
+1 202 263 3325
agetsinger@mayerbrown.com

Endnotes

1 IM Guidance Update 2015-02 (Apr. 2015), *available at* http://www.sec.gov/investment/im-guidance-2015-02.pdf.

2 These discussions were held during the course of the Division of Investment Management's senior level engagement and monitoring efforts.

3 For our summary of OCIE and FINRA's reports on their respective cybersecurity sweep examinations, see http://www.mayerbrown.com/files/Publication/7c1a373a-b348-497b-a6ec-dc9dde98d1be/Presentation/PublicationAttachment/51746088-fdfa-4aa4-abc8-8b49c5cb80f7/150325-UPDATE-Privacy.pdf. For OCIE's report on its cybersecurity sweep examinations of advisers and broker-dealers, see OCIE, National Exam Program, Risk Alert: Cybersecurity Examination Sweep Summary (Feb. 3, 2015) [hereinafter OCIE Risk Alert], *available at* http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf?_cldee=aGFubmFoLndlaW5zdG9jay1nYWxsYWdoZXJAY29yZGl1bS5jb20%3D&urlid=1. For FINRA's report on its cybersecurity sweep examination of broker-dealers, see FINRA, Report on Cybersecurity Practices (2015) [hereinafter FINRA Report], *available at* https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf (the sweep examination report released by FINRA).

4 *See generally* Cybersecurity Roundtable, SEC, https://www.sec.gov/spotlight/cybersecurity-roundtable.shtml (last updated Jan. 16, 2015).

5 The IM Staff made it clear that the measures described in the guidance are recommended only to the extent that they are relevant to the particular firm. They are not intended to be comprehensive and other measures may be better suited depending on the operations of a particular investment company or adviser. The IM Staff stated that each investment company or adviser should determine whether these or other measures need to be considered in connection with addressing cybersecurity risks.

6 The IM Staff mentioned the following control systems and methodologies: user credentials, authentication and authorization methods, firewalls, tiered access to sensitive information and networks, network segregation and system hardening.

7 OCIE observed that nearly all of the advisers examined during the cybersecurity sweep examination use encryption. OCIE Risk Alert, at 4.

8 For a more substantive discussion of these listed measures, see pages 5 to 6 in our legal update, *OCIE and FINRA Announce the Results of Cybersecurity Initiatives* (Mar. 2015), *available at* http://www.mayerbrown.com/files/Publication/7c1a373a-b348-497b-a6ec-dc9dde98d1be/Presentation/PublicationAttachment/51746088-fdfa-4aa4-abc8-8b49c5cb80f7/150325-UPDATE-Privacy.pdf.

[9] Outside resources mentioned in the IM Staff's guidance include: vendors, third-party cybersecurity specialists, publications and conferences, and information sharing networks (e.g., the FS-ISAC). Information sharing networks are, as OCIE observed during its cybersecurity sweep examination, rarely used by advisers, who more frequently relied on discussions with peers, conference attendances, and independent research. OCIE Risk Alert, at 3–4.

[10] During its cybersecurity sweep examination, OCIE observed that a majority of the examined advisers already had written cybersecurity policies and procedures and conducted periodic audits to evaluate their compliance with those policies and procedures. *Id.* at 2.

[11] See 1940 Act Rule 38a-1 and Advisers Act Rule 206(4)-7(a). Also, see *Questions Advisers Should Ask While Establishing or Reviewing Their Compliance Programs*, SEC.GOV (May 2006) [hereinafter Establishing/Reviewing Compliance Programs], http://www.sec.gov/info/cco/adviser_compliance_questions.htm.

[12] *See id.*; *see also Information for Newly-Registered Investment Advisers*, SEC.GOV, http://www.sec.gov/divisions/investment/advoverview.htm (last modified Nov. 23, 2010). Regulation S-P generally requires SEC-registered advisers and (registered or unregistered) broker-dealers and investment companies to adopt policies and procedures to safeguard customer information and records (i.e., insuring security and confidentiality, guarding against threats to the information, and preventing unauthorized access to customer information). *See* Privacy of Consumer Financial Information (Regulation S-P), Release Nos. 34-42974, IC-24543, IA-1883 (June 22, 2000), *available at* https://www.sec.gov/rules/final/34-42974.htm; *see also* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999). Regulation S-ID requires certain SEC-registered advisers, broker-dealers and investment companies to establish an identity theft red flags program designed to detect, prevent, and mitigate identity theft. *See* Identity Theft Red Flags Rules, Release Nos. 34-69359, IA-3582, IC-30456 (Apr. 10, 2013), *available at* https://www.sec.gov/rules/final/2013/34-69359.pdf.

[13] The IM Staff stated that fraud by insiders must be addressed by investment companies pursuant to 1940 Act Rule 17j-1 (prohibiting fraudulent, deceptive, or manipulative acts by investment company personnel) and by advisers pursuant to Advisers Act Rule 204A-1 (requiring advisers' code of ethics to establish a standard of business conduct for their supervised persons).

[14] *See* IM Guidance Update 2015-02, at 5 n.10. For advisers, the IM Staff cited a 2003 rulemaking release which stated that an adviser's fiduciary duty includes the obligation to take steps to protect clients' interests from being placed at risk as a result of the adviser's inability to provide advisory services and that an adviser which actively manages clients' accounts would ordinarily place clients at risk if the adviser ceased operations. *See* Compliance Programs of Investment Companies and Investment Advisers, 68 Fed. Reg. 74,714, 74,716 n.22 (Dec. 17, 2003), *available at* http://www.gpo.gov/fdsys/pkg/FR-2003-12-24/pdf/03-31544.pdf. OCIE observed, during its cybersecurity sweep examination, that slightly more than half of examined advisers have provisions in their business continuity plans that address the mitigation of and recovery from a cyber attack. *See* OCIE Risk Alert, at 2.

[15] If a shareholder of an open-end investment company initiated a transaction to redeem his or her shares in that investment company and an ensuing cyber attack prevented the investment company from processing and redeeming the shares on a timely basis or from calculating NAV, the investment company may be in violation of 1940 Act Section 22(e) and/or Rule 22c-1 thereunder.

[16] OCIE Risk Alert, at 4.

[17] According to OCIE's cybersecurity sweep examination, very few advisers incorporated cybersecurity provisions into vendor or business partner contracts, despite the fact that such entities pose a cybersecurity risk. *Id.*

[18] An SEC investor bulletin provides examples of the types of education material that investment companies and advisers should consider providing to their clients. *See* SEC, *Investor Bulletin: Protecting Your Online Brokerage Accounts from Fraud*, INVESTOR.GOV (Feb. 3, 2015), http://investor.gov/news-alerts/investorbulletins/investor-bulletin-protecting-your-onlinebrokerage-accounts-fraud. According to OCIE, most of the advisers that it examined during the cybersecurity sweep examination offered their clients educational materials about reducing cybersecurity risk and did so through website postings, e-mails, newsletters, and/or bulletins. OCIE Risk Alert, at 4.

[19] *Id.* at 5.