New SEC Cybersecurity Guidance

What it means for fund managers

BRIAN T. DALY, MARC E. ELOVITZ, ROBERT R. KIESEL, HOLLY H. WEISS, MICHAEL L. YAEGER, SCHULTE ROTH & ZABEL

Cybersecurity continues to be a priority for the Securities and Exchange Commission (SEC). The SEC's Office of Compliance Inspections and Examinations conducted a cybersecurity "sweep" examination in 2014 and released a summary of its results in early 2015.

The SEC's Division of Investment Management — which regulates investment companies and investment advisers — has now issued additional cybersecurity guidance in the form of a Guidance Update.[1]

Most registrants will find the Guidance Update to be fairly broad and high-level. It does, however, provide more detail on what reasonable security measures are than the SEC has previously offered, and it expressly confirms that mishandling cyber risks can result in violations of the securities laws by investment companies and investment advisers.

The legal, compliance and information security officers of private and registered fund managers should review this guidance and determine what additional measures within their organization are warranted.

Cybersecurity guidance

The Guidance Update sets forth a three-step approach for registered advisers and investment companies to consider:

1. Assess threats, vulnerabilities and defensive measures currently in place;
2. Design a strategy to prevent, detect and respond to cybersecurity threats; and
3. Implement that strategy through written policies and procedures, internal personnel training and external client education.

Periodic assessments

For the first step, the Division recommends that a fund or adviser consider periodically assessing "the nature, sensitivity and location of information" that it "collects, processes and/or stores" along with "the technology systems it uses." Notably, this recommendation is not limited to investors' personal information but instead extends to all of a firm's data and intellectual property.

Such an assessment amounts to maintaining a detailed inventory and understanding of a firm's cyber infrastructure, including physical devices, the software platforms and applications used on the network, network resources, connections, and "data flows (including locations where customer data is housed)."[2]

The Division also suggests that firms include four additional elements in any cybersecurity assessment:

- Internal and external cybersecurity threats, vulnerabilities of the firm's information and technology systems;
- Currently existing security controls and processes;
- The impact of the firm's information or technology systems becoming compromised; and
- The effectiveness of the firm's governance structure in the context of managing cybersecurity risk.

While the content of this portion of the Guidance Update does not materially extend beyond the implications of the April 2014 risk alert,[3] it provides a standard for a firm's assessment and a lexicon for its defense. As the SEC examination staff likely will incorporate this guidance into their efforts, many managers may want to expressly employ this standard and vocabulary in their next annual compliance review.

A prevention, detection and response strategy

In the second step of the Guidance Update's approach, the Division goes further than the earlier risk alerts in listing specific techniques to consider using in a strategy to "prevent, detect and respond to cybersecurity threats."[4] These include:

- Data encryption;
- Firewalls;
- Restricting the use of removable storage media (e.g., flash drives);
- Deploying software that monitors technology systems for unauthorized intrusions;
- Network segregation; and
- "System hardening."[5]

The Division also encourages firms to broaden the ways that they gather information on cyber threats and suggests that they might do so by engaging "third-party contractors specializing in cybersecurity and technical standards," learning from "topic-specific publications and conferences," and "participating in the Financial Services—Information Sharing and Analysis Center (FS-ISAC)."[6]

This aspect of the Guidance Update provides compliance officers with a framework to present to a firm's internal or external technical consultants and — again, by setting out a relatively specific list of techniques — presents benchmarking criteria that many compliance officers will want to utilize in reviews of their firms' cybersecurity strategy.

Implementation

The third step of the Guidance Update is interesting for its mix of conventional and new guidance. The Division suggests that the cybersecurity strategy be implemented through "written policies and procedures and training … to officers and employees[.]" This is relatively generic guidance that applies to, and has been given in, numerous situations.

What is notable in the Guidance Update is the fairly strong recommendation to "educate investors and clients about how to reduce their exposure to cyber security threats concerning their accounts."

Policy and operational integration

In the Guidance Update, the Division expressly recognizes the need to treat cybersecurity as a thematic issue and not as a policy to be isolated. The Guidance Update specifically identifies identity theft ("red flags"), data protection,

operational controls and business continuity as related concepts that require an integrated cybersecurity defense effort. This endorsement of an integrated approach suggests that firms should undertake a comprehensive review of their compliance manuals to identify policies or procedures that should be tailored.

The Division also notes expressly that this effort will require a holistic approach in terms of personnel and organizational responsibilities; the Guidance Update specifically contemplates involvement of both compliance and operations functions. In addition, the Guidance Update reminds advisers and funds that this is not solely an internal effort.

It states that firms and funds should look at third-party vendors and products and "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."[7]

Potential liability

The Guidance Update expressly contemplates that liability may result from a failure to "tak(e) appropriate precautions concerning information security."[8]

In framing this discussion, the Division states that "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," citing as support anti-fraud and fiduciary rules under both the Investment Company Act and the Investment Advisers Act.[9]

The Division's statement is especially striking given that some courts have held that negligence is sufficient to ground some claims under these acts.[10]

Underscoring this implication of liability for failing to prepare thoroughly for cybersecurity challenges, the Guidance Update closes with this statement:

"Appropriate planning to address cybersecurity and a rapid response capability may, nevertheless, assist funds and advisers in … complying with the federal securities laws."

Next steps for advisers

It is clear from the Guidance Update that the Division is raising the bar for registered advisers and funds in the area of cybersecurity. Greater effort is expected, more tailoring is required and better training is mandated. Falling short could potentially result in liability under the federal securities laws.

Many (or most) advisers and funds simply will not be able to handle all of this internally. Managers are likely to need help from security and cybersecurity experts (for tasks such as penetration testing and vulnerability analyses) as well as from legal and compliance experts. **THFJ**

> "The Division expressly recognizes the need to treat cybersecurity as a thematic issue and not as a policy to be isolated."

Schulte Roth&Zabel
New York | Washington DC | London | www.srz.com

1. Securities and Exchange Commission, Division of Investment Management, IM Guidance Update (April 2015), No. 2015-02, "Cybersecurity Guidance".
   The SEC is not alone in its concerns; other financial regulators have spoken on cybersecurity issues. For example:
   FINRA issued a relatively lengthy report on cybersecurity in February of this year. See Financial Industry Regulatory Authority, Report on Cybersecurity Practices (February 2015); and
   The Commodity Futures Trading Commission staff has also issued guidance on best practices in information security (which included certain cybersecurity measures). See CFTC Letter 14-21 (26 February 2014). The CFTC staff has recommended actions such as the use of encryption and biannual third-party system testing.
2. Securities and Exchange Commission, Office of Compliance Inspections and Examinations, Risk Alert: OCIE Cybersecurity Initiative (15 April 2014) ("April 2014 Risk Alert"), Appendix at 3, Question 1. The SEC released a summary of the results of its Cybersecurity Initiative in early 2015. See Securities and Exchange Commission, Office of Compliance Inspections and Examinations, Risk Alert: Cybersecurity Examination Sweep Summary (3 February 2015) ("February 2015 Risk Alert"). See also our 4 Feb 2015 Alert addressing the February 2015 Risk Alert, "SEC Cybersecurity Update: OCIE Risk Alert Provides Insights for Private Fund Managers on SEC Cybersecurity Examinations."
3. See, e.g., April 2014 Risk Alert at 2 ("As part of this initiative, OCIE will conduct examinations of more than 50 registered broker-dealers and registered investment advisers focused on the following: the entity's cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain cybersecurity threats.")
4. Cybersecurity Guidance at 2.
5. "System hardening" is defined to mean "removing all non-essential software programs and services, unnecessary usernames and logins," and "ensuring that software is updated continuously."
6. Guidance Update at 4 n.6.
7. *Id.* at 5 n.12.
8. *Id.* at 5 n.9.
9. *Id.*
10. *SEC v. Capital Gains Research Bureau*, 375 U.S. 180 (1963) (holding that a violation of § 206(2) may rest on a finding of simple negligence); SEC v. Steadman, 967 F.2d 636,637 (D.C. Cir. 1992) (noting that a violation of § 206(4) does not require that the defendant acted with scienter).