Bloomberg BRIEF

Financial Regulation

10.23.15
FRIDAY

GUEST COMMENTARY

Securities, Futures Regulators Increase Scrutiny, Expectations on Cybersecurity

Financial regulators are emphasizing the risk poor cybersecurity poses to market integrity and financial stability, and elaborating on policies and controls they expect the firms they oversee to have in place, according to **Schulte Roth & Zabel LLP** attorneys **Brian T. Daly, Marc E. Elovitz**, **Robert R. Kiesel**, **Holly H. Weiss**, **Jacob Preiserowicz** and **Michael L. Yaeger**. The attorneys say this means more scrutiny and increased expectations from regulators.

Investment managers' responsibility for cybersecurity has grown like compound returns. Every year brings developments that build on prior obligations. Today, investment managers are subject to more scrutiny and increased expectations from regulators, especially in the securities and futures markets.

Investment advisers have long had privacy obligations (e.g., Regulation S-P, promulgated in 2003). Managers also have long-standing regulatory mandates (under the Security and Exchange Commission's Rule 206(4)-7) to adopt and implement written policies and procedures reasonably designed to prevent violations of the Investment Advisers Act, and in 2013 these regulations were expressly interpreted by the SEC staff to require robust disaster recovery programs. Similar obligations apply under the rules of the Commodity Futures Trading Commission and the National Futures Association, or NFA (the self-regulatory organization for the futures industry). In 2015, the SEC, the CFTC, and the NFA all extended this regulatory trend and deemed cybersecurity compliance and controls to now be core responsibilities of investment managers.

The SEC's Office of Compliance Inspections and Examinations disclosed that its examination staff would be testing investment advisers to assess cybersecurity procedures and controls; CFTC Chairman Timothy Massad stated that cybersecurity was "perhaps the single most important new risk to market integrity and financial stability" and that the CFTC was working on a cybersecurity rule proposal; and the NFA proposed an interpretive notice expressly bringing cybersecurity within the supervisory obligations of commodity futures advisers.

The OCIE and the NFA guidance, read broadly and taken together, should force managers to ensure that they are taking at least the following steps:

Formal Program

■ All three regulators are expecting managers to adopt and enforce a formal, written cybersecurity or information systems security policy that is reasonably designed to provide safeguards that are appropriate to the manager's business.

Compliance Tip: Managers without a written policy should act quickly to adopt a robust cybersecurity program. However, managers should be wary of wholesale adoption of an outside consultant's form policy, as it may not be sufficiently tailored to the manager's business and risks. To the extent that the SEC, the CFTC or NFA have provided examples of specific elements that they expect to see in a Cybersecurity Policy (e.g., multifactor authentication, dynamic updating of personnel access rights, patch management practices, vulnerability scans and penetration testing), they should be carefully considered.

Governance / Oversight

■ Both inspection regimes require that the cybersecurity policy be approved and monitored by "senior management and boards of directors."

Compliance Tip: Meaningful involvement in oversight is likely to be expected by examiners; managers should be encouraging and documenting — in real time — a more active oversight role by senior personnel of the manager and fund directors. This may mean more briefings and meetings, and more costs.

Risk Assessments

■ The regulators expect managers to assess and prioritize, on an ongoing basis, the risks associated with the use of their information technology systems and to continually tailor and revise their cybersecurity policies.

Compliance Tip: Many managers adopt policies that are well-designed on the date of adoption. Risk assessment, however, should be a continual process; managers should not wait for the annual compliance review to reassess cybersecurity risks. Also, identified and prioritized threats and vulnerabilities should be matched to specific cybersecurity policy elements.

Access Rights & Controls / Data Loss Prevention

■ The SEC is interested in how firms monitor "the volume of content transferred outside the firm" and thereby prevent unauthorized distribution of sensitive information by e-mail, hard copy, physical media or web-based file transfers.

Compliance Tip: Managers should perform an information transfer channel inventory and analysis on a periodic basis and compare the volume of data transmitted (by channel) on a relative basis and over time. Corrective action should be taken to limit or close transmission channels that present an unnecessary or unacceptable risk of theft or loss.

Vendor Management

■ After observing that "[s]ome of the largest data breaches over the last few years may have resulted from the hacking of third party platforms" examiners may focus on an adviser's vendor management.

Compliance Tip: Managers should be performing due diligence of vendors when they are selected, negotiating protections into vendor contracts related to access to firm networks or data, and monitoring vendors after they are on-boarded; this process should be documented.

Response / Recovery

■ The regulatory guidance expresses an interest in past cybersecurity incidents.

Compliance Tip: It is important to contemporaneously document each incident and the manager's response. As this can be challenging for compliance personnel, it underscores the need to partner with the information security staff from as early a point in time as possible.