ALERTS

Cybersecurity Update: Takeaways from OCIE's Examination Initiative and the NFA's Rulemaking Proposal

September 21, 2015

As the end of 2015 approaches, financial regulators continue to emphasize the risk that poor cybersecurity poses to market integrity and financial stability, and to elaborate on the policies, procedures and controls they expect investment advisers, commodity pool operators and registered investment companies to have in place.

In January 2015, the Security and Exchange Commission's Office of Compliance Inspections and Examinations ("OCIE") announced that cybersecurity compliance and controls would be a focus of its examinations in 2015. On Sept. 15, 2015, OCIE issued a Risk Alert providing additional information on its focus and noting that OCIE would be "testing to assess implementation of firm procedures and controls" for cybersecurity.[1] The Risk Alert also includes an appendix with a "sample list of information that [OCIE] may review" in examinations on cybersecurity matters.

Similarly, Commodity Futures Trading Commission ("CFTC") Chairman Timothy Massad noted in his recent keynote speeches that cybersecurity has become "perhaps the single most important new risk to market integrity and financial stability"[2] and that the CFTC was working on a rule proposal related to cybersecurity.[3] On Aug. 28, 2015, the National Futures Association ("NFA"), the self-regulatory organization for the futures industry, submitted to the CFTC a proposed interpretive notice (the "NFA's Proposal") that would apply to NFA Compliance Rules 2-9, 2-36 and 2-49, which generally require firms to diligently supervise their

employees and agents or their businesses.[4] The NFA's Proposal provides cybersecurity guidance and focuses on areas similar to those in OCIE's Risk Alert.

These recent pronouncements are largely extensions of past alerts and guidance,[5] and so will not surprise most registrants. Yet they provide additional detail on particular examples of reasonable security measures. The legal, compliance and information security officers of private and registered fund managers should review this guidance and determine whether additional measures within their organization are warranted.

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

- **Formal Program**. All three regulators are expecting managers to adopt and enforce a formal, written cybersecurity or information systems security policy (a "Cybersecurity 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 program, employing outside consultants if necessary. However, managers should be wary of wholesale adoption of an outside consultant's cybersecurity program, as it may not be sufficiently tailored to the manager's business and risks; active involvement in developing the program is needed to have an effective set of policies and procedures. To the extent that the SEC, the CFTC or the 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 and Oversight**. Both inspection regimes require that the Cybersecurity Policy be approved and monitored by (in OCIE's words) "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, but managers should focus on

fostering a culture of active involvement in and oversight of the cybersecurity program.

- **Risk Assessments** . Both OCIE and the NFA 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 to combat the risks facing the business on the date of adoption. Risk assessment (and responses), however, should be a continual interdisciplinary 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 and 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 email, hard copy, physical media (e.g., hard drives) or web-based file transfers. The SEC is not interested exclusively with personally identifiable information ("PII"), but it emphasizes PII risks.

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," the SEC states that examiners may focus on 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. Managers should also ensure that they have "written contingency plans [with vendors] concerning … issues that might put the vendor out of business or in financial difficulty."

- **Incident Response and Recovery**. In addition to seeking information on policies and procedures, the OCIE and NFA guidance both express interest in information regarding past incidents, actual customer losses, and cybersecurity coverage and claims.

Compliance Tip: Because examiners will be expecting to discuss incident responses, it is important to contemporaneously document each incident and the manager's response. As this can be challenging for compliance personnel without extensive technical training or experience, it underscores the need to partner with the information security staff from as early a point in time as possible.

- **Training** . The OCIE Risk Alert and the NFA guidance both address training. The treatment is brief but is more specific than in any previous alerts or guidance on cybersecurity. OCIE, for example, indicates that it is interested in the firm's "training method (e.g., in person, computer-based learning, or email alerts); dates, topics, and groups of participating employees; and any written guidance or materials provided."

Compliance Tip: Managers should be aggressive in scheduling training sessions and in documenting their use and effectiveness. Thought should also be given to tailoring training by employee function and classification.

Authored by Brian T. Daly , Marc E. Elovitz , Robert R. Kiesel , Holly H. Weiss , Jacob Preiserowicz and Michael L. Yaeger .

If you have any questions concerning this *Alert*, please contact your attorney at Schulte Roth & Zabel or one of the authors.

---

[1] Securities and Exchange Commission, OCIE, "OCIE's 2015 Cybersecurity Examination Initiative," Vol. IV, Issue 8 (Sept. 15, 2015) ("Risk Alert").

[2] Timothy Massad, Chairman, CFTC, Keynote Address Before the Futures Industry Association Boca Conference (March 11, 2015).

[3] Timothy Massad, Chairman, CFTC, Keynote Address Before the Beer Institute Annual Meeting (Sept. 9, 2015). Another CFTC commissioner, Sharon Bowen, suggested that bigger changes may lie ahead when she described "ideas that I think are worth considering if and when we propose a rule on improving system safeguards." These ideas included: (1) requiring

each registrant to designate a Chief Information Security Officer; (2) requiring registrants to file annual or quarterly reports on the state of their cybersecurity program; (3) requiring that registrants report any material cybersecurity event to the CFTC promptly (with an example of reports being made "within minutes of a significant breach"); and (4) requiring an independent audit or annual penetration testing for all registrants. Sharon Y. Bowen, Commissioner, CFTC, Keynote Address Before ISDA North America Conference (Sept. 17, 2015). While some of these proposals are consistent with current best practices, the reporting of any material event "within minutes" would be a new requirement for fund managers.

[4] NFA, National Futures Association: Information Systems Security Programs — Proposed Adoption of the Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs (Aug. 28, 2015) (the "NFA's Proposal").

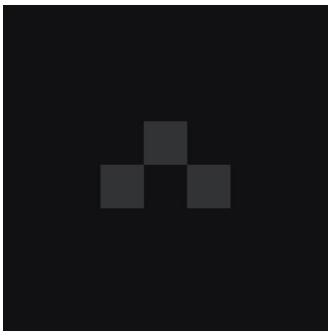
[5] *See, e.g.*, Securities and Exchange Commission, OCIE, Risk Alert: OCIE Cybersecurity Initiative (April 15, 2014), Appendix; SEC, Division of Investment Management, IM Guidance Update (April 2015), No. 2015-02.

Related People

Marc Elovitz

Partner

New York



Holly Weiss

Retired Partner

New York

Jake Preiserowicz

Partner

Washington, DC

Practices

CYBERSECURITY AND DATA PRIVACY

HEDGE FUNDS

INVESTMENT MANAGEMENT

LITIGATION

REGULATORY AND COMPLIANCE

Attachments

Download Alert