Schulte Roth&Zabel

Alert

SEC Cybersecurity Update: OCIE Risk Alert Provides Insights for Private Fund Managers on SEC Cybersecurity Examinations

February 4, 2015

Earlier this week, the SEC's Office of Compliance Inspections and Examinations ("OCIE") issued a Risk Alert[1] providing observations derived from its "Cybersecurity Examination Initiative," which was announced on April 15, 2014. The Risk Alert is based on OCIE's examinations of the cybersecurity policies and practices of 57 registered broker-dealers and 49 registered investment advisers. While the Risk Alert does not provide specific guidance, it does provide fund managers with a snapshot of the cybersecurity practices of broker-dealers and investment advisers[2] and suggests items that are of particular interest to the SEC.

Requirements for Vendors and Other Third Parties

When OCIE announced in April 2014 that it would be conducting its cybersecurity sweep it also issued a "sample" cybersecurity document request to help registrants and their compliance professionals prepare for the examinations.[3] Several of the sweep questions asked registrants to describe precautions taken against cybersecurity risks created by third parties with whom they contract. For fund managers, third parties will often include fund administrators, prime brokers and information technology consultants, among others.

OCIE reports that few investment advisers are placing cybersecurity requirements on vendors they grant access to their firms networks:

- Only 32 percent of the examined sample of investment advisers required such vendors to conduct "cybersecurity risk assessments";[4]
- Only 24 percent "incorporate[d] requirements relating to cybersecurity risk into their contracts" with such vendors;[5] and

[1] Securities and Exchange Commission, Office of Compliance Inspections and Examinations, *Risk Alert: Cybersecurity Examination Sweep Summary* (Feb. 3, 2015) ("Risk Alert"). The SEC also released an investor bulletin — directed at retail investors — that outlines ways that investors can protect themselves against cybersecurity threats.

[2] The 49 examined advisers were (roughly) equally divided into small advisers (under $400 million in assets under management), medium advisers ($401 million to $900 million AUM) and large advisers (over $900 million AUM). In making conclusions about peer performance, however, private fund managers should also note that when the examined entities were categorized by "client concentration," only 14.3 percent were advisers to private funds. In contrast, 67.3 percent of the sample were advisers to retail and individual clients.

[3] *See* Securities and Exchange Commission, Office of Compliance Inspections and Examinations, *Risk Alert: OCIE Cybersecurity Initiative* (April 15, 2014), Appendix .

[4] Risk Alert, at 2.

- Only 13 percent had policies "related to information security training" for such vendors.[6]

In contrast, the numbers for examined broker-dealers were much higher (84 percent, 72 percent and 51 percent, respectively). Given the SEC's consistent focus on the issue of third parties in its cybersecurity risk alerts, investment advisers should consider adding requirements to their contracts.

Appointing a Chief Information Security Officer?
Many of OCIE's sweep questions focused as much on the "who" as the "what." For example, OCIE asked *which specific individuals* (identified by title, department and job function) were responsible for tasks such as:

- Detecting malware;
- Maintaining baseline information about expected events on the firm's network; and
- Monitoring the activity of third-party service providers with access to the firm's network.

OCIE also asked if the firm had a Chief Information Security Officer ("CISO") or equivalent position.

While more than two-thirds of the examined broker-dealers had a CISO, less than a third of the examined advisers did. Instead, OCIE writes, "the advisers often direct their Chief Technology Officer to take on the responsibilities typically performed by a CISO or they have assigned another senior officer (i.e., the Chief Compliance Officer, Chief Executive Officer, or Chief Operating Officer) to liaise with a third-party consultant who is responsible for cybersecurity oversight."[7]

The SEC's focus on this issue suggests that investment advisers should consider whether the size and complexity of their operations and information security risks warrant designating a separate CISO, or the functional equivalent — an employee in charge of information security as distinct from IT operations.

Cyber-Attacks and the Importance of Training
OCIE reports that the majority of cyber-attacks experienced by both broker-dealers and investment advisers are "related to malware and fraudulent emails," and that many of the entities that had financial losses related to fraudulent emails said the losses "were the result of employees not following the firms' identity authentication procedures."[8] In addition, OCIE noted that only a small proportion of broker-dealers and advisers "reported incidents in which an employee or other authorized user engaged in misconduct resulting in the misappropriation of funds."[9]

It is certainly possible that loss to insiders has simply gone undetected, but these reports suggest that for many advisers the risk of loss from the actions of well-intentioned insiders may be more significant than the risk presented by rogue employees. While the statistics may be influenced by the fact that the client base of a supermajority of the examined advisers is individual retail clients, private fund managers

[5] *Id.* at 4.

[6] *Id.*

[7] *Id.* at 5.

[8] *Id.* at 3.

[9] *Id.*

should also focus on training employees and, in particular, training them to recognize and properly deal with potentially fraudulent emails of all kinds (not just redemption requests).

Next Steps

OCIE is careful to note that the SEC staff "is still reviewing the information [obtained in the sweep] to discern correlations between the examined firms' preparedness and controls and their size, complexity, or other characteristics."[10] Further, OCIE states that it "will continue to focus on cybersecurity using risk-based examinations,"[11] and we would expect this to become a part of many standard OCIE examinations.

Authored by Brian T. Daly, Marc E. Elovitz, Robert R. Kiesel, Holly H. Weiss 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.

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

[10] *Id.* at 5.

[11] *Id.*