

SEC Cybersecurity Update

OCIE Risk Alert provides insights for private fund managers on SEC cybersecurity examinations

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

The SEC's Office of Compliance Inspections and Examinations (OCIE) has issued a risk alert providing observations derived from its "Cybersecurity Examination Initiative," which was announced on 15 April 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 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. 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% of the examined sample of investment advisers required such vendors to conduct "cybersecurity risk assessments";
- Only 24% "incorporate[d] requirements relating to cybersecurity risk into their contracts" with such vendors; and
- Only 13% had policies "related to information security training" for such vendors.

In contrast, the numbers for examined broker-dealers were much higher (84%, 72% and 51%, 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."

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."

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."

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 made up of individual retail clients, private fund managers should also focus on training employees and, in particular, training them to recognise 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." Further, OCIE states that it "will continue to focus on cybersecurity using risk-based examinations," and we would expect this to become a part of many standard OCIE examinations.

Schulte Roth & Zabel

Schulte Roth & Zabel LLP
919 Third Avenue, New York, NY 10022
212.756.2000 tel | 212.593.5955 fax | www.srz.com
New York | Washington DC | London