February 2015

Practice Groups:

Investment Management, Hedge Funds and Alternative Investments

Broker-Dealer

Cyber Law and Cybersecurity

Government Enforcement

A Few Takeaways from the OCIE Cybersecurity Examination Sweep Summary

By Mark C. Amorosi, K. Susan Grafton, András P. Teleki

On February 3, 2015, the Securities and Exchange Commission's ("SEC") Office of Compliance Inspections and Examinations ("OCIE") released a Risk Alert (the "2015 Risk Alert") with summary observations from its recently completed cybersecurity sweep examinations of registered broker-dealers and investment advisers. When OCIE announced its cyber sweep initiative on April 15, 2014, its Risk Alert included a sample exam letter that requested, among other things, a detailed summary of all cyber incidents that occurred at the examined firm over the previous year and general information relating to the firm's identification of risks and cybersecurity governance (including a list of the firm's three most serious cybersecurity risks), protection of firm 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 methodology for identifying best practices.

As a result of this initiative, OCIE examined 57 registered broker-dealers and 49 registered investment advisers. Although OCIE does not provide substantive guidance on what broker-dealers and investment advisers should be doing in this area, the 2015 Risk Alert does provide an overview of some broker-dealers and investment advisers' cybersecurity practices. Due to the relatively small number of broker-dealers and investment advisers that were examined (i.e., less than 2 percent of SEC-registered broker-dealers, and less than 1 percent of SEC-registered investment advisers), the 2015 Risk Alert should not be viewed as a summary of industry norms or best practices.

The 2015 Risk Alert is, however, a useful tool for the industry because it summarizes the examined firms' cyber-related practices, and the observations that the staff highlighted provide a window into their focus. The 2015 Risk Alert includes the following key observations:

- The vast majority of examined broker-dealers (93 percent) and investment advisers (83 percent) have adopted written information security policies and procedures, and a large subset of these firms conduct periodic audits to assess compliance with their policies and procedures;
- Written business continuity plans often address the impact of cyber-attacks or intrusions;
- Many firms are utilizing external standards and other resources to model their information security architecture and processes (e.g., the National Institute of Standards and Technology, the International Organization for Standardization, and the Federal Financial Institutions Examination Council);
- The vast majority of examined firms conduct periodic, firm-wide, risk assessments to identify cybersecurity threats, vulnerabilities, and business consequences;

A Few Takeaways from the OCIE Cybersecurity Examination Sweep Summary

- The vast majority of examined firms reported conducting firm-wide inventorying, cataloguing, or mapping of their technology resources;
- Nearly three-fourths of the examined broker-dealers incorporate requirements relating to cybersecurity risk into contracts with their vendors and business partners, but less than one-fourth of the examined investment advisers do so;
- Generally, the examined broker-dealers and investment advisers' written information securities policies and procedures do not address how these firms determine when they are responsible for cyber-related client losses;
- Almost all of the examined broker-dealers and investment advisers utilize encryption in some form;
- Many examined firms provide their clients with suggestions for protecting their sensitive information;
- Generally, in many areas on which the 2015 Risk Alert focused, a higher percentage of the examined broker-dealers than the examined investment advisers had implemented the particular policy or practice identified; and
- Over one-half of the examined broker-dealers maintained insurance for cybersecurity incidents, whereas only a small number of the examined advisers maintained similar insurance.

OCIE further noted that most of the firms subject to the sweep had been the subject of a cyber-related incident either directly or through one or more of their vendors. Significantly, the majority of the cyber-related incidents are related to malware and fraudulent e-mails. Furthermore, one-fourth of the broker-dealers that had losses related to fraudulent e-mails noted that the losses were the result of employees not following the firm's identity authentication procedures.

The sample exam letter, as well as the observations included in the 2015 Risk Alert, could be useful to a firm seeking to evaluate and benchmark its level of preparedness against cybersecurity risks and assist it in developing a cybersecurity program. As noted above, however, we do not believe that the staff's observations should be read as setting forth industry best practices or industry norms. For example, OCIE noted that only five of the examined broker-dealers and four of the examined advisers offered security guarantees to protect their clients against cyber-related losses. The inclusion of this observation may prompt firms to consider whether offering a guarantee is appropriate, but we note that there is no legal requirement to offer such guarantees and such guarantees can significantly increase a firm's potential exposure. One of the key take aways, of course, is that cybersecurity is one of OCIE's top 2015 exam priorities, and that firms registered with the SEC in any capacity, not just broker-dealers and investment advisers, will want to review their preparedness for a cyber exam. The two Risk Alerts provide a good starting point for preparing for such an exam.

As part of K&L Gates LLP's CyberSecurity Task Force, we plan to soon issue an alert on the Financial Industry Regulatory Authority's ("FINRA") report, also released on February 3, 2015, discussing its observations of FINRA member firms' cybersecurity practices. Unlike the 2015 Risk Alert, FINRA included a very detailed and substantive discussion about its expectations with respect to member firms' governance and risk management of cybersecurity, technical controls, incident response planning, vendor management, staff

training, cyber intelligence and information sharing, and cyber insurance. Although the FINRA report is directed to broker-dealers, many of the general constructs discussed throughout the report may be helpful to other securities industry participants that undertake evaluations of their cybersecurity practices.

Authors:

Mark C. Amorosi
mark.amorosi@klgates.com
+1.202.778.9351

K. Susan Grafton
susan.grafton@klgates.com
+1.202.778.9498

András P. Teleki
andras.teleki@klgates.com
+1.202.778.9477

Marguerite W. Laurent
marguerite.laurent@klgates.com
+1.202.778.9403