# Privacy, Data Protection and Cybersecurity Alert

**February 5, 2015**

## SEC Reports Widely Divergent Levels of Cybersecurity Preparedness

This week the U.S. Securities and Exchange Commission (SEC) Office of Compliance Inspections and Examinations (OCIE) announced the results from a sweep of U.S. broker-dealers and investment advisers on cybersecurity. The review of 57 broker-dealers and 49 investment advisers by the Cybersecurity Examination Initiative was initiated last April, with the questions published in an unprecedented risk alert, discussed here. The results from the review are in and although the SEC didn't issue a grade, it appears the broker-dealers were better prepared for cybersecurity risks than the investment advisers.

Not surprisingly, nearly all broker-dealers (88 percent) and investment advisers (74 percent) reviewed had experienced cyber attacks, including fraudulent emails and malware. As a general rule, most broker-dealers (93 percent) and investment advisers (83 percent) had written information security policies in place. Many of these based their security framework on published cybersecurity risk management standards, such as those published by the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO) and the Federal Financial Institutions Examination Council (FFIEC). It is no surprise that third-party risk assessments, reporting and information sharing, and cybersecurity insurance are the most discussed topics in this review.

The most striking weakness was in the area of **third-party risk assessment and procedures**. While firms generally conduct their own risk assessments, fewer firms conduct risk assessments of vendors that have access to their firms' networks, with only 32 percent of investment advisers conducting such assessments. Only 51 percent of broker-dealers and only 13 percent of advisers have policies and procedures related to information security training for business partners and vendors authorized to access their networks. Third-party risk is perhaps the most prevalent concern in cybersecurity, and this review confirms that it is no different for this industry.

The report revealed that there is significant room for improvement in terms of **reporting and information sharing**. Just seven percent of those reviewed reported fraudulent activity to law enforcement or other regulatory agencies, while most reported the activity to the Financial Crimes Enforcement Network (FinCEN). Fewer than half of the broker-dealers participated in information sharing industry groups or organizations, with most participating in the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Finally, the report reveals that there is a wide-ranging approach to **insurance and allocation of loss**. While most broker-dealers have cybersecurity insurance (58 percent), only 21 percent of investment advisers have obtained cybersecurity insurance. Furthermore, allocation of loss appears to be largely unaddressed: very few written policies and procedures address how firms determine whether they are

 

responsible for client losses associated with cyber incidents and even fewer offer guarantees to protect against cyber losses.

The SEC's cybersecurity sweep makes it clear that our nation's broker-dealers and investment advisers are preparing for the new cybersecurity landscape but there are significant opportunities for improvement. Broker-dealers and investment advisers should prepare for an inevitable breach:

- conduct due diligence and audits of third-party vendors
- allocate and mitigate risks through careful contracting with third-party vendors
- evaluate potential cybersecurity insurance coverage
- review activities and risks under NIST or other formal cybersecurity frameworks
- develop and test incident response plans
- review employee training on cybersecurity.

 

## Contact Information

If you have any questions regarding this alert, please contact:

**Michelle A. Reed**
mreed@akingump.com
214.969.2713
Dallas

**David S. Turetsky**
dturetsky@akingump.com
202.887.4074
Washington, D.C.

**Jo-Ellyn Sakowitz Klein**
jsklein@akingump.com
202.887.4220
Washington, D.C.

**Natasha G. Kohne**
nkohne@akingump.com
971 2.406.8520
Abu Dhabi

**Joseph Boryshansky**
jboryshansky@akingump.com
212.872.1054
New York

 