Client Alert

February 5, 2015

SEC Reports the Result of its Cybersecurity Sweep of Broker-Dealers and Investment Advisers

By Jay G. Baris

An SEC cybersecurity sweep examination by the SEC's Office of Compliance Inspections and Examinations (OCIE) found that 88 percent of the broker-dealers (BDs) and 74 percent of the registered investment advisers (RIAs) they visited experienced cyber-attacks directly or indirectly through vendors, the SEC reported in a February 3, 2015 Risk Alert.

The sweep found that while the vast majority of all BDs and RIAs have adopted written information security policies, the SEC staff found some gaps in cybersecurity protection among many firms. BDs and RIAs will find the report useful reading to help them learn how they compare to their peers in their development of cybersecurity procedures. Indeed, the OCIE Risk Alert reminds firms that cybersecurity is one of OCIE's 2015 exam priorities.

For those registered firms looking ahead to their next examination, OCIE's release also provides a hint of how it will focus its efforts in future reviews on the adequacy of a firm's policies and procedures.

OCIE's examination results highlight the magnitude of the issues and challenges that firms face when establishing cybersecurity procedures. While it is not surprising that so many BDs and RIAs have experienced cyber-attacks, it is a somber reminder that systems are vulnerable. Moreover, OCIE reports that more than half of the BDs, and almost half of the RIAs they examined reported receiving fraudulent emails seeking to transfer client funds. Over a quarter of the BDs reported losses related to fraudulent emails, but no single loss in excess of $75,000.

For its sweep, OCIE examined 57 registered BDs and 49 registered RIAs in order to "discern basic distinctions among the level of preparedness of the examined firms."

THE GOOD NEWS

OCIE reported that:

- 93 percent of BDs and 83 percent of RIAs examined have written information security policies.
- Nearly as many of the firms have written business continuity plans that address mitigating the effects of a cybersecurity incident and/or outline the firm's plan for recovering from such an incident.
- A similar number of firms conduct periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences.
- Almost all firms have conducted a firmwide inventory of their technology resources, including physical devices and systems, software platforms, network resources, connections to firm networks from external sources, and hardware, data, and software.
- Almost all firms use encryption.
- While 65 percent of the BDs examined offer their customers online access to account information, all of them provide their customers with information about reducing cybersecurity risk in conducting business with the

firm. And, while 26 percent of RIAs that primarily advise retail clients and provide online access to account information, only three-quarters of those tell their customers how to reduce cybersecurity risks.

- Most of the BDs, and a little over half of the RIAs use published cybersecurity risk management standards, such as those published by the National Institute of Standards and Technology.

ROOM FOR IMPROVEMENT

OCIE also reported findings that indicated that many firms still have a ways to go in developing cybersecurity procedures, or bringing their existing procedures up to snuff.

- Only 72 percent of the examined firms incorporate cybersecurity requirements into their contracts with vendors and other business parties, and only 24 percent of RIAs do so.
- Only 51 percent of firms have procedures related to information security training for vendors or business partners.
- Very few firms address how they determine whether they are responsible for client losses resulting from cyber incidents.
- A little over half of the BDs, and only 21 percent of RIAs, have cybersecurity insurance.
- Only about two-thirds of the BDs, and less than a third of RIAs, have a designated Chief Information Security Officer (CISO).

OUR TAKE

It is always helpful to use industry-wide survey-type information from a regulator to benchmark your firm against the general population of firms. Additional useful information will be available if FINRA releases the results of its separate cybersecurity survey of BDs.

It is not completely clear from the OCIE Risk Alert whether the rates of favorable performance that it found in different aspects of cybersecurity are satisfactory, or if nothing short of 100% success will do. Clearly, registered firms have come a long way, and it's fair to ask in what areas of good cybersecurity housekeeping do the regulators expect 100 percent compliance, and in what areas are these goals more aspirational. Findings in specific exams this year will help calibrate that message; we can hope that the regulators' exam findings will recognize that firms have come a long way, but might still need time to bring all of their procedures up to the state of the art standards.

OCIE's Risk Alert did not indicate whether it found any lapses that could lead to enforcement proceedings or whether the staff will recommend new rules to the SEC. Stay tuned for developments in these areas.

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.