Client Alert

August 15, 2017

OCIE Provides Insight into Issues Identified in Recent Cybersecurity Sweep

By Kelley A. Howes and Jay G. Baris

The National Exam Program of the SEC's Office of Compliance Inspections and Examinations (OCIE) recently published its observations from the second generation of its Cybersecurity Initiative. It reported overall improvement in firms' cybersecurity awareness and preparedness, but said there is plenty of room for improvement. The staff noted that many firms have failed to adopt procedures reasonably tailored to their specific needs, and identified how firms can develop a more robust control environment.

OCIE examined 75 firms, including broker-dealers, investment advisers, and registered funds. It said that it conducted more validation and testing of the firms' policies and procedures than during prior cybersecurity examinations and focused its testing on: (1) governance and risk assessment; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response.

IDENTIFIED IMPROVEMENTS AND CONTINUING AREAS OF CONCERN

The biggest improvement since OCIE's first cybersecurity sweep is that all of the broker-dealers and registered funds, and a vast majority of the advisers that were examined maintained written policies and procedures addressing the protection of customer records and personally identifiable information. The staff said, however, that simply adopting general policies was not best practice since compliance policies and procedures, including those related to cybersecurity, should be reasonably tailored to a firm's business. The staff said that policies and procedures that provide only general guidance, identify limited examples of safeguards, are very narrowly scoped or vague, or don't include implementing procedures, do not meet this standard.

The staff also said that, in some instances, firms did not appear to adhere to or enforce their own cybersecurity policies and procedures. For example, the staff identified instances where policies required ongoing reviews to determine whether certain security protocols were appropriate, but such reviews were performed only annually or not at all. Similarly, the staff raised concerns about firms that adopted policies requiring that all employees complete cybersecurity awareness training, but failed to enforce this requirement.

The SEC staff also reported that nearly all broker-dealers and most of the advisers and funds conducted periodic risk assessments of their critical systems to identify cybersecurity weaknesses, and many conducted penetration tests and vulnerability scans on critical systems. The staff noted, however, that high-risk observations identified during such tests were not consistently remediated.

According to OCIE, all of the broker-dealers and nearly all the advisers and funds that were examined had a process in place for ensuring regular system maintenance, including installation of software patches. However, the staff said that many firms fail to timely test and install such patches. The staff recommended that firms adopt

patch management policies including, among other things, procedures for beta testing a patch with a small number of users and servers before deploying it across the firm, requiring an analysis of the problem the patch was designed to fix, potential risk involved in applying the patch, and the method to use in applying the patch.

RECOMMENDED BEST PRACTICES

OCIE identified several best practices for ensuring that cybersecurity policies and procedures reflect robust controls. These include:

- maintaining a complete inventory of data, information, and vendors, along with a related classification of risks and vulnerabilities;
- maintaining detailed cybersecurity-related procedures, including:
    - instructions for penetration tests;
    - policies and procedures related to granting, modifying, and rescinding access rights; and
    - specific action plans in the event that sensitive information is lost, stolen, or unintentionally disclosed;
- maintaining prescriptive schedules for testing data integrity and vulnerabilities;
- establishing and enforcing controls related to accessing data and systems and the acceptable use of such data; and
- instituting mandatory employee training.

OCIE also noted that an engaged senior management team was important to a robust cybersecurity program.

OUR TAKE

Cybersecurity continues to be a key compliance risk for firms and a high priority examination topic for the SEC, and developments in this area move quickly. Thus, although firms should keep the various factors identified by OCIE's staff in mind when assessing and modifying their cybersecurity policies and procedures, firms also need to carefully consider the profile of their own business, and the rapidly changing cyber environment in which their business is conducted, when adopting and refining their cybersecurity policies and procedures.

Contacts:

Hillel T. Cohn
(213) 892-5251
hcohn@mofo.com

Kelley A. Howes
(303) 592-2237
khowes@mofo.com

Matthew J. Kutner
(212) 336-4061
mkutner@mofo.com

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 13 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.