MorrisonCohen LLP
Law Firm to the Middle Market®

Client Alert

SEC's New Alert Emphasizes Strict Compliance to Narrowly Detailed Cybersecurity Policies for SEC Registered Firms

August 23, 2017 – Reiterating guidance it has already given repeatedly, the Securities and Exchange Commission warned the financial services industry that cybersecurity policies and procedures must be detailed and narrowly tailored to a firm's specific business and investment process and strictly complied with. The adoption of generic or vague policies, or a firm's failure to rigorously enforce stronger ones will be considered violations by the Office of Compliance Inspections and Examinations of the firm's compliance duties.

In a risk alert released earlier this month, OCIE determined that a significant number of SEC registered firms continue to fall short in both the nature of their cybersecurity policies and in the responses they have designed to remedying defects and security flaws that may result.

The SEC staff, drawing on data from their examinations of 75 SEC registered firms, including broker-dealers and investment advisers, highlighted the hallmarks of a strong and robust cybersecurity compliance program, including maintenance of an inventory of data, information and vendors, highly detailed cybersecurity-related instructions, maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities, established and enforced controls to access data and systems, mandatory employee training and an engaged senior management.

While noting that the vast majority of firms maintained written policies addressing cybersecurity related concerns, the Staff found that the policies were frequently contradictory, confusing or not specific enough to help the employees of the firm effectively implement them. The Staff also found that the firms tested their systems much less frequently than the policies required and that deviations from policies, such as failing to train employees and lack of system maintenance exposing firms to Regulation S-P privacy concerns, were not being remedied as quickly as they should. Finally, while the majority of broker-dealers had prepared procedures for data breach incidents and notifying client of such incidents, less than two-thirds of investment advisers had similar procedures in place.

The Staff focused its inquiry primarily on the strength of each firm's policies and how closely they were in fact followed, specifically in governance and risk assessment, access rights and controls, data loss prevention, vendor management, training and incident response. Although the SEC had conducted a similar fact-finding exercise in 2014, the newer examination, called the Cybersecurity 2 Initiative, probed more deeply into each firm's cybersecurity policies, procedures and controls, noting that while generally firms had improved their cybersecurity platforms, there was still a good deal of room for improvement.

The Staff, however, did not make specific recommendations or identify specific best practices. It seems likely that with cybersecurity continuing to be a top priority for the SEC examination staff, guidance will come through enforcement procedures. The compliance professionals of all regulated firms should consistently be reviewing their firm's policies and systems and to ensure effectiveness and proper implementation.

For further information regarding this and/or any other compliance issue, please contact:

Jessica Colombo
(212) 735-8752
jcolombo@morrisoncohen.com

David Lerner
(212) 735-8609
dlerner@morrisoncohen.com