CORPORATE COUNSEL

SEC Preps Cybersecurity Exams for Wall Street Firms

Rebekah Mintzer, Corporate Counsel
April 23, 2014

Is the securities industry ready for a cybersecurity checkup? The data doctor is in. The Office of Compliance Inspections and Examinations (OCIE) of the U.S. Securities and Exchange Commission has announced that more than 50 lucky broker-dealers and investment advisers will have to submit to exams from the agency to evaluate the health of their defenses against cybercrime.

In a recent risk alert [PDF], the OCIE laid out its exam criteria, indicating the office's interest in several aspects of cybersecurity preparedness, including

company policies, remote customer access and breach-detection systems. The move, one of several that the SEC has made in the cybersecurity area, underscores the abundance of cyberthreats at work in the financial sector.

The decision to examine cybersecurity practices in this part of the securities industry didn't come out of thin air. "I'm not surprised at all," Tracy Gerber, a comanaging shareholder at Greenberg Traurig's offices in West Palm Beach, Fla., told CorpCounsel.com. "There's been increasing regulatory focus on the cybersecurity issue for sometime now."

The SEC held a roundtable on cybersecurity in March, and in 2011 it issued informal guidance on disclosures in relation to cyberrisks and incidents. There are no formal cybersecurity guidelines from the SEC or the Financial Industry Regulatory Authority, which Gerber believes is likely because both the technology and threats have evolved quickly. However, she thinks there may be some formal guidelines on the horizon—while noting that a broader approach based more on guidance and less on hard rules would be the better way for agencies to go because business needs and risk profiles vary.

"Every firm is different," she said. "Firms cater to different types of clientele that have different types of usage of online services, and firms need to have the flexibility to tailor the way they address cybersecurity threats to their business."

The examination criteria issued by the OCIE covers a lot of ground—and provides a set of parameters for broker-dealers and investment advisers to look at while planning and evaluating the safety of their data systems. The exam asks about firms' identification of cybersecurity risks, including questions about network mapping and the frequency of risk assessments. It asks how networks are protected, including whether they conform to the framework recently released by the National Institute of Standards and Technology (NIST) [PDF], how the firm handles threat detection, and the level of risk posed by fund transfers and third-party vendors.

With all of the sensitive data that securities firms handle every day, said Gerber, there are bound to be dangers, whether these are insider threats, hackers or outsiders who would use customer data to swipe someone's identity.

The SEC exam contains, for example, a section dealing with third parties and vendors, which Gerber said most broker-dealers and investment advisers make use of. "Anytime you have a third-party vendor who has access to your system, there's a concern because you're expanding the access to your firm's operational system to someone who is not a member of your firm," she noted.

To combat these issues, Gerber said, many in the financial-services industry have already made rules to limit their exposure to cybercrime and data theft. For example, some are forgoing email for delivering trade or wire instructions, and others are adding a more detailed authorization process for third-party logins.