PUBLICATION

SEC Cybersecurity Roundtable Addresses Broker-Dealer and Investment Adviser Risks

April 21, 2014

On March 26, 2014, the Securities and Exchange Commission (SEC) hosted a roundtable to discuss cybersecurity issues facing public companies, broker-dealers, investment advisers and other market participants. The roundtable included representatives from both the public and private sectors, and participants discussed the nature and scope of cyberattacks, the growing cybersecurity community and novel issues facing members of the securities markets today. The roundtable also included comments from members of the Financial Industry Regulatory Authority (FINRA), which included cybersecurity threats as a key component in its 2014 exam letter.

Although cybersecurity has become a major topic of discussion, since 2011, the SEC has provided only informal guidance to registrants and other market participants. Those informal comments relate primarily to disclosure obligations in reports, which focus on potential threats to the registrant's business and preventative measures meant to protect investors. But in light of recent, high-profile cyberattacks (e.g., Target's December 2013 data breach), the SEC has acknowledged the lack of formal guidance for members of the securities markets. SEC Chairwoman Mary Jo White remarked that "[t]he SEC's formal jurisdiction over cybersecurity is directly focused on the integrity of our market systems, customer data protection, and disclosure of material information. But it is incumbent on every government agency to be informed on the full range of cybersecurity risks and actively engage to combat those risks in our respective spheres of responsibility."

Commissioner Luis Aguilar stated that while the SEC must play a key role in the area of cybersecurity, "what is less clear is what that role should be." Notably, Commissioner Aguilar pitched an idea for a cybersecurity "task force" composed of members from each of the SEC's divisions to review cybersecurity threats and provide timely advice to the SEC.

Last month's roundtable signaled that expanding monitoring and disclosure efforts related to cybersecurity is a major priority for the SEC. Accordingly, market participants should expect continued guidance and scrutiny from SEC examiners for issues relating to cyberattacks and cybersecurity.

Discussion at the roundtable also centered on the landscape and forecast for cybersecurity relating to market participants, namely registered investment advisers and broker-dealers. Daniel Sibears, the executive vice president of regulatory operations and shared services at FINRA focused primarily on three major areas of risk for market participants: (1) operational risks (technology failures, external events and internal control failures); (2) insider risks in connection with rogue employees; and (3) outsider risks, such as hackers invading technology systems. Additionally, Sibears warned of growing "phishing attacks" against clients, where personal data is misappropriated in order to make transfers out of a client's account. Other participants echoed Sibears' assessment, adding that malware was a major concern for broker-dealers, and other data breaches and identify theft vulnerabilities.

Roundtable participants were hopeful that the SEC would provide "principles-based guidance due to the constantly changing landscape" rather than a rigid rules-based approach. Sibears also noted that FINRA would likely "push out some effective practices" moving forward, and acknowledged the need for adaptation in the ever-changing cybersecurity landscape.

As the SEC and FINRA move forward with cybersecurity efforts, market participants should adhere to several best practices, with participants listing multifaceted control procedures, risk-based approaches, continual monitoring efforts and adoption of a "culture of cybersecurity" into daily business practices among them. One participant concluded that market participants should expect attacks, take preventative measures, monitor ongoing threats and plan for contingencies and remediation. As rule-makers consider recent cybersecurity events and a renewed call for guidance, investment advisers should expect a fuller review of their cybersecurity risks, data privacy and information security resources, policies for prevention, detection, and response to cybersecurity attacks, policies for cybersecurity education and IT training, identity theft plans and business continuity plans, while FINRA will likely apply similar pressure on broker-dealers by reviewing their cybersecurity policies, procedures and internal controls.

On April 15, 2014, the SEC advised that it would begin moving forward with its cybersecurity initiatives, including examinations and reviews of broker-dealer and investment advisers. The SEC will focus on the areas of cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain cybersecurity threats. Market participants can expect the SEC to release additional guidance throughout 2014.

If you have questions regarding cybersecurity issues facing public companies, broker-dealers, investment advisers, and other market participants, or need assistance in evaluating your company's policies and procedures, please contact an attorney in Baker Donelson's Broker-Dealer/Registered Investment Adviser Group.