Advisory

MARCH 2014

If you have any questions about this Advisory, please contact:

RICHARD LEVAN
215.988.8316
rlevan@wiggin.com

ELISE GARBER
215.988.8314
ebarger@wiggin.com

SEC Holds Roundtable on Cybersecurity

On March 26, the Securities and Exchange Commission (SEC) held a roundtable discussion regarding the issues and challenges that cybersecurity presents for market participants and public companies. The roundtable was divided into four panels, discussing in turn the cybersecurity landscape generally, cybersecurity disclosure issues faced by public companies, cybersecurity issues faced by exchanges and other key market systems, and how broker-dealers, investment advisers, and transfer agents address cybersecurity. As Acting Senior Director for Cybersecurity Programs of the National Security Council for The White House, Ari Schwartz summed up the current cybersecurity risk landscape, "This is not really a problem that you are going to get past, but a problem that you have to manage."

Generally, each panel centered on cybersecurity preparedness. The themes that were continuously touched on by each panelist included coordination and communication between and among the government and the private sector, understanding threat vectors, how to stay current, and the disclosure process. As explained during the preliminary panel by Cyrus Amir-Mokri, Assistant Secretary for Financial Institutions for the Department of the Treasury, a partnership between and among the public and private spheres of the financial world "brings the whole picture together." Amir-Mokri explained that the private sector is the frontline defense, as they are in the best position to manage defense of their systems, while the government has certain capabilities to provide technical and other assistance. He went on to state that the entire effort to manage cybersecurity risk "requires everyone to cooperate and coordinate," and "that is what we work on every day."

Regarding the maintenance of an up-to-date and effective cybersecurity system, Mark Graff, Chief Information Security Officer for NASDAQ OMX, noted that threat modeling and risk assessments are necessary. Expounding upon the issue of internal threats, Graff declared that it is "not enough to bet on your own employees, because we are in trust relationships with so many other companies, vendors, and third parties." He discussed the trading ecosystem with brokerage houses and other exchanges, which allows the circulation of information that must be protected. As noted by David G. Tittsworth, Executive Director and Executive Vice President of the Investment Adviser Association, risks to the financial sector come in three categories: (1) individual money management, where account takeover is the number one risk (i.e. identify and account theft); (2) institutional money management, where hacktivism is feared (denial of service attacks, state-sponsored terrorism, and systemic threats); and (3) for both kinds of firms, internal risks (i.e., a rogue employee or a lost laptop).

Daniel M. Sibears, Executive Vice President of Regulatory Operations/Shared Services at FINRA, explained that cybersecurity is a "key area of concern on the regulatory

CONTINUED ON NEXT PAGE

© 2014 Wiggin and Dana LLP In certain jurisdictions this may constitute attorney advertising.

SEC Holds Roundtable on Cybersecurity CONTINUED

side." Sibears discussed a sweep that FINRA recently launched in order to get a cross-section of issues that financial firms are facing, including types of threats, vulnerabilities, use of information technology, and government involvement. Sibears noted that thus far, the three key areas that firms have been reporting as hot issues are: operational risks, insider employee threats, and external hackers penetrating their systems. The goal for this latest sweep is to "push out effective practices from FINRA" in order to respond to the rapidly changing environment. As Craig Thomas, Chief Information Security Officer of Computershare, stated, "Technology moves faster than security," and the panelists all advocated for a joint, private- and public- sector effort in order to manage the increasingly changing cybersecurity landscape.

The SEC is still grappling with what to do next. SEC Commissioner Luis Aguilar, who organized the Roundtable, said that the Commission should establish a cybersecurity task force with participation and members from each of the Commission's key divisions. Aguilar explained that "given the extent to which the capital markets have become increasingly dependent upon sophisticated and interconnected technological systems, there is a substantial risk that a cyberattack could cause significant and wide-ranging market disruptions and investor harm." The Panelists continued to debate the level and form of guidance that the SEC should provide.

Time will tell whether SEC regulation of cybersecurity issues will be rules- or principles- based. As both the SEC and FINRA listed cybersecurity as one of their top exam issues for 2014, cybersecurity risk and preparedness will continue to be a substantial concern for the financial industry moving forward.

This publication is a summary of legal principles. Nothing in this article constitutes legal advice, which can only be obtained as a result of a personal consultation with an attorney. The information published here is believed accurate at the time of publication, but is subject to change and does not purport to be a complete statement of all relevant issues.