Ted Dahlstrom
Federal Agency Hearing Recap writing sample

Subject: A Securities and Exchange Commission roundtable discussion on cybersecurity

Introduction

The SEC held a cybersecurity roundtable discussion today at its headquarters. All five Commissioners were in attendance, along with about 100 people in person and many more watching online. The roundtable was the idea of Commissioner Luis Aguilar, who originally proposed it last year. The SEC held the event in order to "discuss the cybersecurity landscape and cybersecurity issues faced by exchanges and other key market systems, broker-dealers, investment advisers, transfer agents, and public companies." Additionally, panelists were invited to "discuss industry and public-private sector coordination efforts relating to assessing and responding to cybersecurity issues."

Notable Remarks

During her opening remarks, Chair Mary Jo White remarked that the SEC places the threat of cybersecurity as the most pressing threat facing the agency, even more important than terrorism. Soon, she said, the government will spend more on cybersecurity than on fighting terrorism. She also said that a proposed rule related to cybersecurity policy for SROs, Reg SCI, will be completed later this year. Additionally, Commissioner Luis Aguilar remarked that the SEC should create a cybersecurity task force to advise the financial services industry on relevant issues.

Cyrus Amir-Mokri, Assistant Treasury Secretary for Financial Institutions, mentioned in his opening statement that Treasury, the White House, and the National Institute of Standards and Technology (NIST) break cybersecurity policy down into three categories: 1) Resilience, or how firms protect themselves by internal IT activity and information sharing among each other and the government; 2) Incident Management, including how the government and private companies manage a cybersecurity attack; and 3) Recovery, or how both the government and industry respond in the wake of a cybersecurity attack. His remarks came at the beginning of the first panel, which addressed the general cybersecurity landscape.

Issues facing derivatives industry

Issues facing OCC and the derivatives industry were addressed in the third panel, which discussed Market Systems. **James Burns**, Deputy Director of SEC's Division of Trading and

Markets moderated the panel. The panelists were **Mark G. Clancy**, Managing Director and Corporate Information Security Officer, The Depository Trust and Clearing Corporation (DTCC); **Mark Graff**, Chief Information Security Officer, NASDAQ OMX; **Todd Furney**, Vice President, Systems Security, Chicago Board Options Exchange; **Katheryn Rosen**, Deputy Assistant Secretary, Office of Financial Institutions Policy, Department of the Treasury; **Thomas Sinnott**, Managing Director, Global Information Security, CME Group; and **Aaron Weissenfluh**, Chief Information Security Officer, BATS Global Markets, Inc.

In her opening remarks, Ms. Rosen noted that the FSOC oversees cybersecurity for the administration and considers it a top priority. She mentioned that "cyber hygiene" is very important for companies and that the global regulatory community is addressing cybersecurity issues, with the SEC taking a lead role. IOSCO is also working on principals for financial infrastructure. President Obama's recent Executive Order put forward ideas on how firms should address cybersecurity issues, and the administration is continuing to pay a lot of attention to the issues. She believes that government must share information with the private sector and vice versa. The declassification of government documents is needed, as is government access to sensitive private sector information.

The other panelists discussed how they combat cyber threats. Their actions include loss scenarios, threat modeling exercises and extensive testing of both internal controls and penetration attempts. Testing is also important to find out if the system they built is designed as intended. Investments in cybersecurity infrastructure include internal staff and third-party experts, along with a security-oriented culture that includes internal structures designed to prevent employees from abusing their access to sensitive information. Last year, the entire financial services industry participated in Operation Quantum Dawn, which was a test of the industry response to multiple cyber attack scenarios.

Cooperation between government and industry

Mr. Graff brought up what would happen if a trade that was hacked came to Nasdaq from a broker-dealer. He said that, under current policies, Nasdaq does not have the authority to break the trade. He requested further guidance on such a scenario from the SEC. Mr. Furney said that CBOE has the authority to break such a trade, but agreed that additional guidance would be helpful. Mr. Clancey expounded by explaining that, while "self-help" rules are understood, what if a big attack caused everyone to declare at once? Parity in the markets is essential, and cyberattacks raise many systemic risk policy issues. They are still exploring solutions.

Ms. Rosen later reiterated her point that communication between the financial services sector and the government is essential. The networks must speak to each other. It is important for the private sector to give information to the government so it has all the information necessary to connect the dots in case a cyberattack is affecting a different industry, such as the energy markets. It is also important to publicly disclose cyberattacks so the public can protect themselves. Mr. Weissenfluh responded by saying that BATS discloses information through FSSCC and also regularly interacts with the other exchanges.

Mr. Clancy concurred, agreeing that the best way to mitigate risks is to share information in real time. Mr. Furney added that the DHS and FBI have been good at sharing information with CBOE over the past "one or two" years. Mr. Graff said that many exchanges, including Nasdaq, use FSISAC to communicate with each other and the government and also use the World Federation of Exchanges to communicate with overseas exchanges.

Conclusion

The last topic was whether there were any best practices being used by the exchanges. Mr. Graff mentioned that "853" is a good standard baseline. Further research revealed that he was likely referring to NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations." According to NIST, "the document is considered a principal catalog of security standards and guidelines used by federal government agencies that NIST is required to publish by law." In other words, it is an official government document intended to provide guidance on how federal agencies protect their information and information systems. Here is a press release about the document: http://www.nist.gov/itl/csd/sp800-022812.cfm

While the White House EO and NIST frameworks have been helpful, the exchanges agree that there is no common set of cybersecurity guidelines in use today.