The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

**MEMO# 28003**

March 28, 2014

# Summary of the SEC's March 26 Cybersecurity Roundtable

[28003]

March 28, 2014

TO: TECHNOLOGY COMMITTEE No. 4-14
COMPLIANCE MEMBERS No. 6-14
CHIEF RISK OFFICER COMMITTEE No. 4-14
RISK ADVISORY COMMITTEE No. 2-14 RE: SUMMARY OF THE SEC'S MARCH 26 CYBERSECURITY ROUNDTABLE

This memo summarizes the discussion of the panelists at the Cybersecurity Roundtable that the SEC held on March 26, 2014. [1] The Roundtable began with opening remarks by Chair Mary Jo White and Commissioner Luis Aguilar. Chair White noted in her remarks that cyber threats "are first on the Division of Intelligence's list of global threats, even surpassing terrorism." She also noted that the SEC's "formal jurisdiction" over cybersecurity is "directly focused on the integrity of our market systems, customer data protection, and disclosure of material information." According to her, the purpose of the Roundtable was to better inform the SEC, the market place, other government agencies, and the private sector regarding what the risks are and how best to combat them. In his opening comments, Commissioner Aguilar noted that he had suggested to Chair White that the SEC hold the Roundtable to explore, among other issues, what the SEC should be doing in response to growing concerns with cybersecurity. Both Chair White and Commissioner Aguilar attended the entirety of the Roundtable and asked questions of the panelists throughout. [2]

The Roundtable was comprised of four panels comprised of private industry and government agency or SRO representatives and moderated by an SEC staff person. The four panels, each of which is briefly summarized below, were: the Cybersecurity Landscape; Public Company Disclosure; Market Systems; and Broker Dealers, Investment Advisers, and Transfer Agents. The Roundtable touched on a variety of topics and was very informative. [3] Of note, several panelists stated that the financial services industry does "a great job" in this area. In part, however, that is because the industry is a prime target for cybersecurity attacks and this necessitates the industry having detection and defense systems that are as advanced as practicable. With respect to the role of the SEC in cybersecurity, panelists noted, among other things: the fact that cybersecurity is a serious concern does not mean the SEC needs to be doing anything in response; should the SEC decide to do something, they need to make sure that it is principles based and not

prescriptive and they need to avoid requiring disclosure that could inadvertently increase a registrant's vulnerability; and the SEC should attempt to facilitate discussions between government agencies and the industry to better alert the industry to cybersecurity concerns.

## Panel I: The Cybersecurity Landscape [4]

[Moderators: Thomas Bayer, SEC CIO; Keith Higgins, Director, Division of Corporate Finance; and James Burns, Deputy Director, Division of Trading and Markets]

This panel discussed the current cybersecurity landscape including who the "bad actors" are, the methods they utilize to extract information, what is being done in response, and the importance of sharing threat information. The points made by panelists included the following:

- The threat vector includes criminals, nation states, hacktivists, [5] and terrorists, each of which have their own agenda and their motives influence the types of attacks they conduct. The methods they use include Distributed Denial of Service (DDoS) attacks; kidnapping data and holding it for ransom; misappropriating intellectual property; compromising systems; and stealing non-public personal information (NPPI). A person under attack needs to know where the threat is coming from and the attacker's motive because not all attacks are equal and different attacks have different consequences. A firm's incident response plan needs to address the variety of attacks. While the bad actors attacking the financial service sector are the same types of bad actors attacking other industries, the attacks on financial services firms are evolving faster in response to the evolving security used by financial services firms. One panelist likened cybersecurity threats against financial services firms to the game "Whack-A-Mole" where, as soon as the firm defends against one attack or one type of attacker, another one pops up to take its place.
- While the White House has focused its efforts on protecting the critical infrastructure (which includes the financial services sector), firms must also be cognizant of internal threats (e.g., a compromise of information like that of Edward Snowden).
- The two biggest targets of cybersecurity attacks are financial services firms and energy providers. Financial services firms are targets because of the assets they hold; financial service firms and the energy sector are targets because a massive attack on either would adversely affect our nation's reputation. As mentioned above, in response to its status as an ongoing target, the financial services sector tends to be way ahead of other industries in awareness of and responses to cybersecurity attacks.
- Unlike in the past, attackers today are no longer "drive bys." Instead, they are becoming more patient and deliberate, meaning the attacker can lurk inside a firm's system for months or years before actually attacking or appropriating or exploiting information. It is not unusual for the government to become aware of such a lurking attacker before the company that is the victim of the attack is aware of it.
- With respect to current industry challenges, the panel mentioned the need for the industry to prioritize what systems/information needs to be protected because it is impossible to protect everything all the time. Of particular concern is third party access to systems/information, not only with respect to business partners, but incidental providers that one would not normally think of (e.g., office cleaning services).

- With respect to involvement of boards or senior management in this process, it was noted that they are best suited to ensuring there are company-wide processes in place to assess and respond to threats involving core business activities. According to one panelist, less than 1% of boards have expertise in cybersecurity or technology issues. Questions board may want to ask include: How do we know what data may be leaving the company and how are we monitoring for leakage? Also, does the company have a cybersecurity response plan in place to immediately respond to an incident? Boards may also want to make sure there is a "reporting up" mechanism in place that ensures that all material incidents get to the persons who need to know the information on a timely basis. It was also recommended that firms create a culture that recognizes that every employee presents a potential cybersecurity vulnerability and get away from thinking of cybersecurity as merely a technology issue.

- There was a robust discussion regarding sharing information about attacks and vulnerabilities. Such sharing is crucial to understanding how attacks and attackers are evolving and how to respond. FS-ISAC [6] was cited several times as a great source of information. It was noted that sharing of information among financial services firms still presents challenges because companies do not want to disclose that they have been attacked or what their vulnerabilities are. One panelist noted that no industry participant has a competitive advantage when it comes to cybersecurity. Rather than sharing information, companies seem more focused on containing any information regarding an attack to avoid harming their brand. It was noted that the "bad guys" are great at sharing information with other bad actors so more bad actors can exploit security vulnerabilities. [This difference in sharing approaches between the bad actors and financial services firms was referred to as "information asymmetry."] One challenge that may also impede the sharing of information among companies is knowing who within a company should receive the information. It was recommended that the person charged with this role should have appropriate security clearances to make sure they can receive sensitive information from the government.

## Panel II: Public Company Disclosure

[Moderator: Keith Higgins, Director, Division of Corporation Finance]

Though this panel's focus was on the disclosure of cybersecurity threats and breaches, the panelists discussed a variety of related topics. The panelists' comments included the following:

- Cybersecurity is the number one enterprise-wide risk today. The government tends to have more intelligence regarding attacks and incidents than the private sector. The federal government recently notified 3000 companies that their systems had been breached. (These were not necessarily financial services firms.) For many, this was the first notice they had of the breach. One panelists who represents a cybersecurity insurer noted that his firm has seen a 20% increase in policies over the past year.

- It was noted that the SEC's approach to disclosure of cybersecurity incidents and threats is unique among other industries and regulators. [7] The panel discussed the recent framework published by the National Institute on Standards and Technology ("NIST") and noted that it provides industry the flexibility it needs to design and implement cybersecurity programs. [8] One panelist noted that the NIST framework is very similar to the process used by an underwriter to review a firm that has applied for cybersecurity insurance. Another panelist noted that the SEC's disclosure

requirements – which have, in large part, resulted in boilerplate language – do not have much of an impact on behavior and, because disclosure of breaches can adversely impact a company, companies tend to err on the side of non-disclosure of breaches except as required by state law. [9] It was also noted that more detailed disclosure is not in a company's best interest because it can make the company more vulnerable to attacks. Also, to the extent the company receives classified information from the government regarding an attack, the company may be prevented by law from disclosing such information.

- There was much discussion during this panel regarding board involvement on cybersecurity issues and the fact that there has been a significant increase in board focus on cybersecurity. When asked whether boards should have expertise in this area, it was noted that, depending on the type of business, there may be value in having such expertise. However, it should be remembered that the role of the board is one of oversight and companies tend to be better served by board members who are generalists that can address a variety of business issues. Panelists commented that, to the extent that boards address cybersecurity through a committee, it tends to be the audit committee.
- One panelist cautioned the SEC that, just because cybersecurity is an issue of concern, it does not mean that the SEC should try to regulate in this space. It was also noted that the SEC should not be attempting to influence companies to do more in this space by requiring enhanced disclosure. It was pointed out that enhancing the current disclosure may likely result in merely increasing the amount of disclosure, not the value of such disclosure.

## Panel III: Market Systems

[Moderator: James Burns, Deputy Director, Division of Trading and Markets]

This panel explored cybersecurity from the perspective of the markets and exchanges. Panelists noted the following:

- The focus of the U.S. Treasury in this space is on data integrity, systemic risk from a cybersecurity incident, and customer protection.
- Nasdaq noted that their focus is on the information in their systems someone may be after rather than what type of bad actor may be after the information. Nasdaq also noted the importance of extensively vetting any staff they hire and any vendors they utilize (including the service they hire to take care of their plant and the persons who deliver food and supplies to their cafeteria) to eliminate, to the extent practicable, any internal threats.
- When asked what steps the exchanges take to protect themselves, they responded that they do extensive modeling of threats, testing, and engage in frequent response exercises. Nasdaq mentioned that they also have a "kill switch" on critical systems so they can shut them down immediately if necessary to avoid a contagion. CBOE noted that they incorporate cybersecurity into their enterprise-wide risk program. While they used to report on their efforts to the audit committee of their board, they now report to the full board. The CME noted that it meets with the FBI quarterly to share information on an ongoing basis. The DTCC stated that it tries to build security into each of their systems during the design phase to better protect their interests. The exchanges also noted that they use both internal and external resources to assist them, but over time they are developing far more expertise inside their firms. They

also said that they ability to report information anonymously to the FS-ISAC is beneficial.

- The exchanges also noted that one issue they struggle with is how and when to notify market participants of an incident. Apparently, when an incident occurs, they tend to be far more focused on a return to operations than on making disclosures and prosecuting criminals, which seems to be the focus of federal agencies and regulators.
- In response to a question from Commissioner Aguilar regarding what the SEC can do to help the exchanges, the panelists recommended that the SEC take a risk-based approach to the issue and not a one-size-fits-all because all firms and all risks are different. It was also recommended that the regulators become more knowledgeable about how the exchanges operate and how they approach these issues. The panel also recommended greater collaboration between: (1) the variety of regulators to avoid redundant reviews and inconsistencies; and (2) the regulators and exchanges to prepare for systemic cyber contagion events that may impact multiple exchanges and/or sectors simultaneously.

## Panel IV: Broker-Dealers, Investment Advisers, and Transfer Agents [10]

[Moderators: David Grim, Deputy Director, Division of Investment Management; James Burns, Deputy Director, Division of Trading and Markets; Drew Bowden, Director, OCIE]

This panel discussed cybersecurity concerns in this sector of the industry. The issues discussed during this panel included the following:

- Among advisers, account takeovers (by fraudsters), identity theft, and hacktivism tend to be the greatest concerns. An increasing concern is the vulnerability arising in connection with mobile devices used by employees. One issue firms struggle with after or during an incident is making sure the concern is remediated without adversely impacting customers' activities. Another concern is the lack of internal expertise in this field and the lack of available experts to call on when there is a problem. According to one panelist, there is a huge shortage of cybersecurity experts who focus on incident analysis and response. Smaller firms are likely falling behind larger firms in defending themselves against attacks due to limited resources. Fortunately, however, the threat profile of smaller firms is less than that of larger firms.
- One panelist noted that today they have to consider – and plan for – the threats that are likely to come in 18-24 months because if they do not address those concerns today, they will not be able to protect against them when they hit.
- The panel was asked about best practices relating to cybersecurity. They listed the following:

    - A recognition that there is no one solution to address cybersecurity concerns – protections and responses must be agile and continuously evolving;
    - All firms should presume they will be attacked and should recognize that technology will always advance faster than security;
    - Do not underestimate internal threats;
    - Know the firm's points of vulnerability and take steps to address them;

- If possible, appropriately "wall off" information so an intrusion into one system cannot spread to other systems;
- Make sure the cybersecurity program is deployed enterprise wide and that it continuously evolves to address new vulnerabilities and changing threats;
- Remember that cybersecurity is an enterprise-wide risk impacting all aspects of the firm and not a technology or IT issue;
- The amendments the SEC previously proposed to Regulation S-P (but never adopted) [11] provide good guidance for creating, implementing, testing, and revising security programs; and
- Remember that a company is only as strong as its weakest link. In this regard it was noted that the higher the level of management, the less securely they behave. As a result, senior managers and the C-suite can be the greatest vulnerability in a firm because they either do not think the rules apply to them or they do not want to be inconvenienced by the security protections.

- When asked what the SEC should be doing relating to cybersecurity, the panelists offered the following suggestions:

  - The SEC could issue principles-based guidance rather than prescriptive rules that will become outdated before they are adopted. It was mentioned that Canadian authorities went the prescriptive-rule approach and this has impeded the ability of financial firms in their cybersecurity efforts;
  - The SEC should consider adopting the amendments previously proposed to Regulation S-P;
  - The SEC should facilitate the sharing of information by or among registrants without exposing such registrants to regulatory actions;
  - The SEC should work with FINRA to publish a document, similar to the joint document published in the wake of Hurricane Sandy, regarding beneficial practices in this area;
  - The financial services regulators should work together to avoid inconsistencies and redundancies;
  - The SEC should focus on outcomes and work with the industry to get to the right result rather than approaching this from an enforcement perspective; [12] and
  - When the SEC promulgates any new regulatory requirement, it should consider whether the rule could inadvertently expose a registrant to increased cybersecurity vulnerabilities.

Tamara K. Salmon
Senior Associate Counsel

**endnotes**

[1] The agenda for the Roundtable, which includes a list of each panel's moderator(s) and panelists is available at http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370541253749#.UzXPDTfN8f

R. An archived webcast of the four and one-half hour Roundtable is available at: http://www.sec.gov/news/otherwebcasts/2014/cybersecurity-roundtable-032614.shtml.

[2] Commissioners Gallagher, Piwowar, and Stein attended portions of the Roundtable.

[3] The SEC is also seeking public comment on issues raised during the Roundtable including the SEC's efforts in this space. See http://www.sec.gov/spotlight/cybersecurity-roundtable.shtml.

[4] Though this panel was scheduled to last an hour, it was the longest panel of the day and lasted closer to 90 minutes.

[5] A "hacktivist" is a person who engages in hacktivism. According to Wikipedia, hacktivism, which is a portmanteau of hack and activism, is the use of computers and computer networks to promote political ends, including free speech, human rights, and information ethics.

[6] FS-ISAC is an acronym for the Financial Services – Information Sharing and Analysis Center. According to the website for FS-ISAC, it was established in 1999 by the financial services sector in response to 1998's Presidential Directive 63. That directive, which was later updated by 2003's Homeland Security Presidential Directive 7, mandated that the public and private sectors share information about physical and cybersecurity threats and vulnerabilities to help protect the U.S. critical infrastructure. The ICI has been a participant in FS-ISAC since its inception. More information about FS-ISAC is available on FS-ISAC's website: https://www.fsisac.com/.

[7] In 2011, the SEC's Division of Corporate Finance issued guidance regarding the disclosure of cybersecurity events. See http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. This guidance states, in part, that "registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky." Such disclosure should include a "discussion of the registrant's business and operations that give rise to material cybersecurity risks and the potential costs and consequences," a "description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences," and "risks related to cyber incidents that may remain undetected for an extended period." It additionally notes that, for those firms that have been a victim of malware, "the registrant may need to discuss the occurrence of the specific attack and its known and potential costs and other consequences."

[8] In February, NIST released the "Framework for Improving Critical Infrastructure Cybersecurity" (the "NIST Framework"), which was created through collaboration between industry and government. The NIST Framework consists of voluntary standards, guidelines, and practices to promote the protection of critical infrastructure. It is expected that, at some point, federal agencies may mandate use of the NIST Framework.

[9] It was also noted that the state laws that require disclosure are limited to disclosure of breaches that involve accessing non-public personal information of consumers or investors. If the breach relates to intellectual property or the theft of proprietary information, it likely is not required to be disclosed. One panelist also noted that disclosure of a breach is more likely to adversely impact a company's reputation than its stock price and, if the stock price is impacted, it tends to be a temporary impact.

[10] In response to a request from the SEC staff, the ICI arranged for Mark Manley, the CCO of AllianceBernstein, to represent our industry on this panel.

[11] See Regulation S-P, Privacy of Consumer Information and Safeguarding Personal Information, SEC Release No. 34-57427 (March 4, 2008), which is available at: http://www.sec.gov/rules/proposed/2008/34-57427.pdf. The Institute filed a comment letter that supported the SEC's proposal but recommended clarification of some of the proposal's provisions.

[12] Related to this issue, one panelist, John Reed Stark, who previously spent almost 20 years with the SEC's Enforcement Division, including as the Chief of the Office of Internet Enforcement, commented on his concern with the ability of registrants to meet the standards of the module the SEC is using in their cybersecurity reviews of registrants. He said he has "serious concerns" with the SEC making enforcement referrals of firms that do not measure up. In the absence of any fraudulent activity, he said the SEC's focus should not be on enforcement but on helping the firms to comply and address any deficiencies in their cybersecurity efforts.

---