Published on *The National Law Review* https://natlawreview.com

SEC (Securities and Exchange Commission) Hosts Roundtable on Cybersecurity Issues and Challenges

Article By:

Susan D. Resley

Linda L. Griggs

Sean M. Donahue

Participants recognize the importance of board oversight and risk disclosures.

On March 26, the U.S. Securities and Exchange Commission (SEC) hosted a roundtable to discuss cybersecurity and the issues and challenges it raises for market participants and public companies.[1] The participants included senior SEC staff, other high-ranking government officials from various agencies, and industry leaders from the private sector. All five SEC commissioners attended the roundtable and engaged actively in the dialogue with roundtable participants. Two of the commissioners' opening statements are posted on the SEC's website.[2]

Each of the SEC commissioners and the SEC staff participating in the roundtable expressed their beliefs that the SEC plays an important role in the cybersecurity arena. In her opening statement, Chair Mary Jo White said 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." The SEC did not explain the scope of its jurisdiction and did not use the roundtable to update or clarify the guidance issued by the SEC's Division of Corporation Finance in October 2011 regarding cybersecurity disclosure (the 2011 Disclosure Guidance).[3] Nor did the SEC participants indicate that new guidance would be forthcoming. Instead, the roundtable focused on collaborative solutions to address cybersecurity issues and the SEC's potential role in this area. The agenda topics included the cybersecurity landscape, public company disclosure, market systems, and broker-dealers, investment advisers, and transfer agents.

SEC's Involvement with Cybersecurity Issues

The 2011 Disclosure Guidance was the SEC's first official commentary on the issue of when and how a registrant should disclose the risks of a cyber attack and the consequences of an actual cyber attack. Since the publication of the 2011 Disclosure Guidance, a flurry of events has transpired, repeatedly drawing the SEC's attention to this complicated and ever-developing topic. For example, in April 2013, Senator John D. Rockefeller (D-WV) sent a letter to the SEC, requesting further

guidance on disclosure obligations regarding cybersecurity risks and cyber incidents and elevation of this SEC staff guidance to the Commission.[4] SEC Chair White responded to Senator Rockefeller's letter in May 2013, emphasizing the need to disclose cybersecurity risks under existing disclosure requirements, as explained in the 2011 Disclosure Guidance.[5] Her letter also pointed out that the SEC staff had issued comment letters to approximately 50 companies concerning compliance with the 2011 Disclosure Guidance. She further noted that the SEC's Division of Corporation Finance is actively engaged in addressing cybersecurity matters. In March 2014, senior SEC staff from the Office of Compliance Inspections and Examinations (OCIE) indicated that OCIE is developing a way to test the preparedness of investment advisers and investment companies for cyber breaches.

Actual cybersecurity breaches at major corporations have also resulted in an increased focus by the public on cybersecurity issues. Most recently, major cybersecurity breaches at several retailers, banks, and other companies drew public attention to the vulnerability of companies and the consequences of a cyber incident. All of these events led to the SEC's decision to host the cybersecurity roundtable.

The Cybersecurity Roundtable

One goal of the cybersecurity roundtable was to discuss the SEC's role in this area. In his opening remarks at the roundtable, Commissioner Luis A. Aguilar made it clear that "[t]here is no doubt that the SEC must play a role in this area. What is less clear is what that role should be."

Consistent throughout the roundtable were several key messages, including the following:

- **Board of Directors' Involvement:** Cybersecurity is a threat that necessitates the involvement of every level of a company, especially the board of directors, but exactly how that responsibility should be allocated and the level of necessary expertise may depend on the industry and other considerations.

- **Public Disclosure:** Companies must disclose cybersecurity threats and incidents, but when and how is currently unclear, and the SEC is wrangling with this ever-developing issue. For example, Chair White stated that the 2011 Disclosure Guidance "makes clear that material information regarding cybersecurity risks and cyber incidents is required to be disclosed," while Commissioner Kara M. Stein questioned whether materiality was the right standard for cybersecurity disclosures. Thus, appropriate disclosures about cybersecurity risks and breaches may require (1) more SEC guidance, (2) an SEC requirement, or (3) continuing SEC staff comments.

- **Information Sharing:** Sharing information among companies and with the government is essential in preventing cyber attacks. The government can assist in this effort by acting as a clearinghouse to receive and disperse information about cyber incidents to companies, by defining the legal protections covering such information and by giving the private sector the appropriate clearances for access to classified information.

- **Preparation:** Companies must be prepared to defend against and respond to cyber attacks on a timely basis. Adequate preparation includes performing tests and risk assessments daily, quarterly, and annually and developing playbooks defining response plans for breaches.

- **Government Guidelines:** Government guidance on disclosure and standards that can be implemented by companies to prevent cyber attacks are helpful, but prescriptive rules are not

beneficial, given the changing and dynamic landscape of cybersecurity and the likelihood of having outdated rules.

Importance of the Board's Oversight

The role of the board of directors received considerable attention and involved, among other things, discussion about the following:

- The need to appoint a board member with cybersecurity expertise, which may depend on the type of company and its dependence on information technology. For example, although the panelists consistently praised the finance industry as a leader in cybersecurity, the risks faced by that industry, as well as the potential consequences of an attack, necessitate leadership because the nature of the industry's information and products is dependent on technology. This industry-specific distinction might demand the appointment of a specific board member responsible for overseeing these issues.

- The need for directors to seek to understand the nature, consequence, and extent of cyber breaches, as well as why the company was targeted and the strategic implications of the breach.

- The board committee that may be charged with oversight of a company's cybersecurity efforts, recognizing that board involvement in oversight of cybersecurity is also critical. A recent survey showed that 50% of the boards surveyed had a risk committee. According to participants in the roundtable, most risk committees oversee cybersecurity risks. Oversight of cybersecurity issues may also reside with the audit committee because of stock exchange rules that require audit committee oversight of risk assessment and risk management.

Disclosure of Cyber Risks

SEC representatives and other industry representatives at the roundtable addressed the following issues concerning disclosure of risks and attacks:

- The suitability of the current materiality standard. Commissioner Stein made comments suggesting that disclosure might be necessary, despite the lack of materiality, because of the unique nature of cybersecurity. SEC Chair White did indicate, however, that materiality is the current standard.

- The tremendous disincentive to disclose a cyber breach because of reputational and litigation risk absent an affirmative disclosure obligation under state law or the federal securities laws.

- The need for company-specific risk-factor disclosure, as opposed to generic disclosure similar to that of a company's peers, and whether the 2011 Disclosure Guidance has simply resulted in boilerplate risk-factor disclosure.

- Whether the SEC has given issuers enough guidance regarding cybersecurity disclosures or whether the SEC should adopt certain minimum disclosure requirements, perhaps by industry, or principles-based requirements and whether the SEC's disclosure guidance or requirements can be as dynamic as the cybersecurity landscape.

- The benefits of additional SEC guidance on cybersecurity, as opposed to the improvement of cybersecurity disclosure practices through the comment-letter process.

Top Issues Companies Should Consider

- Companies should view cybersecurity as a problem to manage and detect on a timely basis because it may not be avoidable. Cyber incidents are nondiscriminatory, and successfully handling cybersecurity issues necessitates the involvement of the board of directors, senior management, and lower-level employees.

- Companies should consider implementing a multilayered approach to cybersecurity, where it is not just the job of one person or department within an organization, but the job of the entire organization from the top down.

- Boards of directors should be actively focused on cybersecurity issues. They should consider whether they need to nominate a director that has cybersecurity expertise and whether a board committee should have initial oversight responsibility and, if so, which committee. They should also consider whether any additional steps are needed to ensure that they are satisfying their fiduciary oversight duties, particularly given that at least one derivative action involving a cybersecurity breach has been filed claiming a breach of fiduciary duty by the board for, among other things, failing to take reasonable steps to maintain customers' personal and financial information and failing to implement any internal controls designed to detect and prevent a data breach.

- Companies should review their disclosures about cybersecurity risks and their implications and make sure that they are company-specific, without adversely affecting their ability to protect themselves from cyber attacks. In evaluating the disclosures, companies should view the requirement for material disclosures as encompassing qualitative and quantitative factors, including the possible impact on a company's reputation.

- Companies should evaluate their disclosure controls and procedures to determine whether they are designed to effectively enable them to evaluate the need for appropriate disclosures about cybersecurity risks and implications. For example, risk factors should reflect all of the implications of a cyber incident, including the impact of such an incident on the company's reputation. In addition, the requirement that the management discussion and analysis cover any trend or uncertainty that is reasonably likely to have a material effect on the company's results may require a company to discuss the implications of a cyber incident.

- Companies should consider whether controls relating to the risks of cyber attacks may be mandated by the requirements in Section 13(b)(2)(B)(iii) of the Securities Exchange Act of 1934, as amended (the Exchange Act), and Rule 13a-15(f) thereunder that a company's internal control over financial reporting include controls to safeguard assets. Controls to safeguard assets must "provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition" of such assets. Companies should consider whether the identities of customers and perhaps other forms of customer data, though not all, could be considered assets for purposes of Section 13(b)(2)(B)(iii) and Rule 13a-15(f) of the Exchange Act. For example, intangible assets on a company's balance sheet that relate to customer relationships might be assets subject to the requirement in Section 13(b)(2)(B)(iii) and Rule 13a-15(f).

We will continue to monitor the issuance of any additional guidance in this area, whether issued by the SEC or another governmental entity.

---

[1]. An archived webcast of the March 26 roundtable is available here.

[2]. View SEC Chair Mary Jo White's opening statement here and Commissioner Luis A. Aguilar's opening statement here.

[3]. *See* Div. of Corp. Fin., SEC, CF Disclosure Guidance: Topic No. 2 Cybersecurity (Oct. 13, 2011), *available* here.

[4]. *See* Letter from Senator John D. Rockefeller to SEC Chair Mary Jo White (Apr. 9, 2013), *available* here.

[5]. *See* Letter from SEC Chair Mary Jo White to Senator John D. Rockefeller (May 1, 2013), *available* here.

National Law Review, Volume IV, Number 90