SEC MAKES CLEAR THAT CYBERSECURITYIS A FOCUS AREA

By Susan D. Resley, Linda L. Griggs, Sean M. Donahue, Kate M. Emminger and Jenny Harrison

The threat of a cybersecurity attack looms larger than ever. Almost every month, a new incident is announced, with innumerable consumers affected. Since 2011, these incidents have drawn increasing attention from the U.S. Securities and Exchange Commission ("SEC") as it considers steps it should address in this area, including whether companies should enhance their disclosure about potential threats and past incidents. The topic has been especially highlighted this year, with the SEC hosting a roundtable to address the issue, and subsequent Commissioner statements reiterating the roundtable themes.

I. SEC First Addresses Cybersecurity Issues in 2011

The 2011 disclosure guidance, issued by the staff of the SEC's Division of Corporation Finance, was the staff'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.[1] 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.[2] SEC Chair Mary Jo 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.[3] 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.

Recent major cybersecurity breaches at several retailers, banks, and other companies have drawn 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.

II. The Cybersecurity Roundtable Demonstrates Further SEC Interest

On March 26, 2014, the SEC hosted a roundtable to discuss cybersecurity and the issues and challenges it raises for market participants and public companies.[4] 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. Chair 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 2011 disclosure guidance. 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.

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, butwhen and how is currently unclear, and the SEC is wrangling with this ever-developing issue.

- **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.

III. 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.

IV. 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 Kara 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.

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

V. Continued Attention to Cybersecurity

A. SEC Attention

In the few short months after the roundtable, the SEC continues to prioritize and emphasize cybersecurity issues. On April 15, OCIE released a Risk Alert announcing a cybersecurity initiative focusing on preparedness for the capital markets themselves.[5] OCIE will assess potential weaknesses and risks by examining over 50 registered broker-dealers and investment advisers. Attached to the Risk Alert was a seven page sample request for information and documents that OCIE plans to utilize to obtain the proper information from examined registrants.

On June 10, Commissioner Aguilar spoke at the "Cyber Risks and the Boardroom" Conference at the New York Stock Exchange.[6] There, Commissioner Aguilar noted that "[a]s an SEC Commissioner, the threats are a particular concern because of the widespread and severe impact that cyber-attacks could have on the integrity of the capital markets infrastructure and on public companies and investors." He focused his remarks on the role of the board of directors, echoing roundtable themes, by reiterating the need for boards to:

- manage cybersecurity along with other traditional risks;

- be educated about cybersecurity;

- clearly designate responsibility for cybersecurity; and

- have a clear crisis response plan.

Commissioner Aguilar also pointed to the February 2014 "Framework for Improving Critical Infrastructure Cybersecurity," released by the National Institute of Standards and Technology ("NIST"),[7] as a voluntary baseline of good practices. Commissioner Aguilar explained that the "Framework encourages companies to be proactive and to think about these difficult issues in advance of the occurrence of a possibly devastating cyber-event … At a minimum, boards should work with management to assess their corporate policies to ensure how they match-up to the Framework's guidelines — and whether more may be needed."

Finally, as the scrutiny surrounding cybersecurity protection increases, SEC enforcement actions based on inadequate anticipation of or response to cybersecurity risks are more likely. These actions could be brought under Regulation S-P (17 CFR § 248.30(a), also called the "Safeguards Rule"[8]). The SEC has brought at least one such action, claiming that the firm's policies did not adequately protect customer information.

B. Other Attention

The SEC is not the only stakeholder addressing cybersecurity issues. Several other developments should give companies plenty of reasons to prioritize cybersecurity. For example, in April, the Department of Justice and Federal Trade Commission issued a joint policy statement assuring companies that sharing information regarding cybersecurity issues will not be considered an antitrust violation.[9] Similarly, in June, Senator Dianne Feinstein and Senator Saxby Chambliss circulated a draft bill proposing various mechanisms to facilitate companies' sharing of information with the government.[10] Also, companies that have cyber attacks are at risk of derivative actions based on such attacks and proxy advisory firm recommendations that shareholders vote against members of a company's audit committee because of the cyber attacks

VI. Top Issues Companies Should Consider

Given cybersecurity threats and the SEC's continued interest in cybersecurity disclosure, companies should consider the following:

- 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 multi-layered 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 two derivative actions involving a cybersecurity breach have 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. Disclosure that a company may face a cyber attack is inaccurate if the company has already experienced a cyber attack. 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, and any necessary updates to the risk factors to reflect any new cyber attacks, 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).

ENDNOTES

1 *See* Div. of Corp. Fin., SEC, CF Disclosure Guidance: Topic No. 2 Cybersecurity (Oct. 13, 2011), *available at* (http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm).

2 *See* Letter from Senator John D. Rockefeller to SEC Chair Mary Jo White (Apr. 9, 2013), *available at* (http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51).

[3] *See* Letter from SEC Chair Mary Jo White to Senator John D. Rockefeller (May 1, 2013), *available at* (http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=7b54b6d0-e9a1-44e9-8545-ea3f90a40edf).

[4] An archived webcast of the March 26 roundtable is *available at* (http://www.sec.gov/news/otherwebcasts/2014/cybersecurity-roundtable-032614.shtml).

[5] *See* OCIE Cybersecurity Initiative (April 15, 2014), *available at* (http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf).

[6] View Commissioner Aguilar's speech transcript at (http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#_ednref1).

[7] View NIST's "Framework for Improving Critical Infrastructure Cybersecurity" at (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf).

[8] View Regulation S-P (17 CFR § 248.30(a)) at (http://www.sec.gov/rules/final/34-42974.htm.).

[9] *See* Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information, *available at* (http://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf.).

[10] *See* Cybersecurity Information Sharing Act, *available at* (http://www.feinstein.senate.gov/public/index.cfm/files/serve/?File_id=08de1c1b-446b-478c-84a8-0c3f35963216).

Susan D. Resley is a Partner with the San Francisco office of Morgan, Lewis & Bockius.

Linda L. Griggs is a Partner with the Washington, D.C. office of Morgan, Lewis & Bockius.

Sean M. Donahue is an Associate with the Washington, D.C. office of Morgan, Lewis & Bockius.

Kate M. Emminger is an Associate with the San Francisco office of Morgan, Lewis & Bockius.

Jenny Harrison is an Associate with the San Francisco office of Morgan, Lewis & Bockius.