McDermott Will & Emery

Public Companies: SEC Issues Guidance on Cybersecurity Disclosures

October 21, 2011

The Guidance addresses a public company's obligation to make certain disclosures concerning cybersecurity risks and cyber incidents.

On October 13, 2011, the Division of Corporation Finance of the U.S. Securities and Exchange Commission (SEC) issued "CF Disclosure Guidance: Topic No. 2 – Cybersecurity" (the Guidance), regarding a public company's obligation to make certain disclosures concerning cybersecurity risks and cyber incidents. The SEC issued the Guidance in apparent response, at least in part, to a letter to the SEC signed earlier this year by five U.S. senators inviting SEC guidance on the topic. Signatories included U.S. Senators John D. Rockefeller, Sheldon Whitehouse, Richard Blumenthal, Robert Menendez and Mark Warner. The senators' letter pointed to, among other things, a 2009 survey in which Hiscox, a cyber-insurance underwriter, found that 38 percent of public companies did not adequately report information about security risks in public disclosures.

Requirement to Disclose Cybersecurity Risk Is Not "New"

The requirement under the federal securities laws to disclose material cybersecurity risks and incidents is not new and should not be viewed as creating additional disclosure obligations. Public companies are currently obligated to evaluate and disclose to investors significant factors that make an investment in the company's securities speculative or risky, events or uncertainties that are reasonably likely to have a material effect on the company's financial results or condition, and any additional information necessary to make the other required disclosures by the company not misleading. (*See, e.g.*, Regulation S-K, Items 503(c) and 303, Securities Act Rule 408, Exchange Act Rule 12b-20, and Exchange Act Rule 14a-9.) In other words, these disclosure obligations already existed, albeit not expressly. By issuing this Guidance, the SEC is signaling to public companies that this is a "hot button" issue in which the investing public is interested. In the wake of some high-profile cyber incidents affecting companies earlier this year, the SEC appears to be using this opportunity to give a

timely reminder to public companies of what is expected under the securities laws in connection with these incidents.

In fact, the SEC has in the past issued interpretive guidance in response to current events that highlight disclosure obligations. For example, in response to heightened public awareness of climate change issues and calls from certain sectors of the investment community, the SEC issued in January 2010 interpretive guidance for disclosure of business and legal developments relating to climate change (Commission Guidance Regarding Disclosure Related to Climate Change). Similarly, after the recent credit crisis, in order to facilitate understanding by investors of the liquidity and funding risks faced by public companies, the SEC issued in September 2010 an interpretive release to improve disclosure of liquidity and capital resources in Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A) contained in public filings (Commission Guidance on Presentation of Liquidity and Capital Resource Disclosures in Management's Discussion and Analysis). Unlike those interpretative releases, the Guidance is a statement of the SEC Staff, the second in a new series of Staff Disclosure Guidance publications, and not of the Commission itself. Although the Guidance is not a rule, regulation or statement of the Commission, public companies should nevertheless ensure that their disclosures and their disclosure controls and procedures comply with the Guidance to the extent applicable to their material cybersecurity risks and any cyber incidents.

Overview of the Guidance

In the Guidance, the Staff notes the following background:

For a number of years, registrants have migrated toward increasing dependence on digital technologies to conduct their operations. As this dependence has increased, the risks to registrants associated with cybersecurity have also increased, resulting in more frequent and severe cyber incidents.

The Guidance notes there are two separate triggers for cybersecurity disclosures. First, public companies must evaluate cybersecurity risks, regardless of whether a cyberattack has occurred, and then assess whether disclosure of those risks is appropriate. For example, companies must evaluate what aspects of business (such as outsourcing) might lead to material cybersecurity risks and then make disclosures of

those risks, including a description of potential costs and other consequences of these risks. Similarly, where a company undergoes an internal audit or risk assessment and uncovers a vulnerability that has the potential to expose the company to a material breach, it may be required to disclose that information. The Guidance makes clear that the Staff does not believe public companies are required to disclose cyber vulnerabilities in a way that could provide a road map for hackers to exploit that vulnerability. "Instead," the Guidance states, "registrants should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant in a manner that would not have that consequence."

A second trigger for disclosure is the occurrence of specific events, including cyber attacks and other cyber incidents. For example, public companies may need to timely disclose information regarding the financial effects of a material breach, whether that breach was caused by an external hacker or by employee oversight. This could include disclosing information about investigation costs and other effects, such as when a cyberattack or breach could:

- Expose a company to a lengthy government investigation and costly third-party claims, including breach of contract claims, credit defaults, regulatory fines and litigation
- Cause significant business interruption and result in lost revenues and impairment of certain assets
- Undermine the value of services
- Harm a company's reputation
- Lead to substantial costs of remediation, including use of internal and external resources, the provision of customer incentives and more

Risk Factors

Item 503(c) of Regulation S-K provides that a public company must disclose the most significant factors that make an investment in the company speculative or risky (see Item 503(c) of Regulation S-K, and Form 20-F, Item 3.D). The Guidance provides that whether those factors include cyber risks depends on the registrant's particular facts and circumstances, when applicable:

cybersecurity risk disclosure provided must adequately describe the nature of the material risks and specify how each risk affects the registrant. Registrants should not present risks that could apply to any issuer or any offering and should avoid generic risk factor disclosure.

In determining whether a cybersecurity risk is significant, public companies should evaluate their cybersecurity profile and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents. Companies should also look at their industry competitors and the known cybersecurity incident history of those competitors.

Among the disclosures that may be appropriate to include are aspects of the company's business that give rise to the cybersecurity risk, risks associated with outsourcing functions, material past cyber incidents (including a description of costs and other consequences) and description of relevant insurance coverage.

Management's Discussion and Analysis of Financial Condition and Results of Operations

A company should include a discussion of cybersecurity risks and incidents in MD&A if such issues have had or are likely to have a material effect on the operations, liquidity or financial condition of the company. For example, if intellectual property is stolen in a cyberattack, the MD&A should describe the property that was stolen and the potential effect of the theft on future revenues, including litigation costs and any expected increase in cybersecurity protection.

Description of Business

If one or more cyber incidents materially affect a company's products, services, competitive conditions, or relationships with its customers or suppliers, then the company should disclose this in its "Description of Business." For example, if a company learns of a cyberattack that could potentially harm a product in development, the company should disclose both the incident and any potential harm to the new product as a result of the incident.

Legal Proceedings

If a company or any of its subsidiaries is a party to any pending material legal proceedings involving a cyber incident, the company should disclose that information in its "Legal Proceedings" disclosure.

Financial Statement Disclosure

The SEC Guidance points out that cybersecurity risk and specific cyber incidents may have a broad impact on a company's financial statement disclosures. Prior to a cyber incident, a company may incur costs related to theft prevention and cyber security. Following a cyber incident, a company may incur additional costs, including:

- Losses from asserted and unasserted claims related to the incident
- Losses from additional customer incentives to mitigate damages in business relationships
- Impairment of such assets as software, trademarks and patents

Companies should therefore ensure that any such specific incident or cybersecurity risk potentially causing a material impact to their financial statements is accounted for and properly disclosed.

Disclosure Controls and Procedures

Companies are required by the SEC to disclose conclusions on the effectiveness of disclosure controls and procedures. A company should therefore consider the risks that cyber incidents may pose to the company's ability to record, process, summarize and report information required in SEC filings. If a cyberattack could potentially prevent the required information to be reported, the company may conclude its disclosure controls are ineffective.

Conclusion

In the wake of this Guidance, we will likely see an uptick in public company disclosures in this area, with respect to both specific cyber incidents that have occurred and risks

that such an incident might occur. As with any other risk, the SEC cautions that such disclosure "should be tailored to [the issuer's] particular circumstances and [should] avoid generic 'boilerplate' disclosure." Any public company that materially relies on online sales, for example, should evaluate whether cybersecurity risks to its business warrant risk factors or other disclosures in its public filings. A company is not required to give a roadmap of its weaknesses, but it may have to disclose if it has a particular weakness given its business model. As a result, companies must balance carefully the need to make a disclosure with the need to protect their cybersecurity vulnerability. Although the SEC cautions against boilerplate disclosures, common themes are likely to emerge nevertheless in cybersecurity disclosures made in issuers' SEC filings in the industries and sectors where cybersecurity issues are most prevalent.