

October 20, 2011

SEC Issues Disclosure Guidance on Cybersecurity Matters and Cyber Incidents

The Securities and Exchange Commission (SEC) Division of Corporation Finance (CF) issued disclosure guidance (“Guidance”) on October 13, 2011, regarding cybersecurity matters and cyber incidents. While the Guidance does not change existing disclosure requirements, it does add specificity to existing requirements. In some respects, that specificity is helpful, but the Guidance fails to take into account the uncertainty that inevitably accompanies efforts to assess and disclose cybersecurity matters and incidents. Below is a summary of the Guidance and our thoughts regarding its effects, including its impact on disclosures both before and after a cyber incident, enforcement-related proceedings and potential litigation.

What is the purpose of the Guidance?

The stated purpose of the Guidance is to assist registrants in preparing disclosures required in registration statements under the Securities Act of 1933 and periodic reports under the Securities Exchange Act of 1934, related to both “cybersecurity risks and cyber incidents.” “In order to maintain the accuracy and completeness of information in effective shelf registration statements, registrants may also need to consider whether it is necessary to file reports on Form 6-K or Form 8-K to disclose the costs and other consequences of *material cyber incidents*.” According to the Guidance, the CF “determined that it would be beneficial to provide guidance that assists registrants in assessing what, if any, disclosures should be provided about cybersecurity matters in light of each registrant’s specific facts and circumstances.”

Although not mentioned in the Guidance, the Guidance follows from an ongoing dialogue between Congress and the SEC related to cyber risks. In a June 6, 2011, letter from SEC Chairwoman Schapiro to the chairman of the Senate Commerce Committee, the chairwoman stated that “as we further analyze [disclosure of information security risks], we will consider your request for interpretative guidance.”

Is the Guidance legally binding?

No. As indicated in the Guidance, and contrary to many commentators’ suggestions, the Guidance “is not a rule, regulation, or statement of the SEC, and the Commission has neither approved nor disapproved its content.” It does, however, provide nonbinding guidance regarding existing disclosure obligations concerning both cybersecurity matters and cyber incidents, and no doubt will be relied upon in enforcement proceedings and by plaintiffs’ counsel in litigation. *See, e.g., In re Heartland Payment Systems, Inc. Securities Litigation*, 2009 WL 4798148 (D.N.J. Dec. 7, 2009) (granting motion to dismiss in securities class action involving disclosures related to a cyber attack against defendant that resulted in the release of payment card data).

What Are Cybersecurity Matters and Cyber Incidents for the Purposes of the Guidance?

While not expressly defined in the Guidance, a reasonable reading of the Guidance would suggest that “cybersecurity matters” are those that involve “cybersecurity,” which the Guidance broadly defines as “the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access. WhatIs?com available at <http://whatis.techtarget.com/definition/cybersecurity.html>. See also Merriam-Webster.com available at <http://www.merriam-webster.com/dictionary/cybersecurity>.” This is a broad definition that places a host of what would normally be considered routine matters within the ambit of the Guidance.

The Guidance similarly defines “cyber incidents” broadly: “[C]yber incidents can result from deliberate attacks or unintentional events,” including, but not limited to, “gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption ... [and] denial of service attacks on websites.” “Cyber attacks may be carried out by third parties or insiders using techniques that range from highly sophisticated efforts to electronically circumvent network security or overwhelm websites to more traditional intelligence gathering and social engineering aimed at obtaining information necessary to gain access.” “The objectives of cyber attacks vary widely and may include theft of financial assets, intellectual property, or other sensitive information belonging to registrants, their customers, or other business partners. Cyber attacks may also be directed at disrupting the operations of registrants or their business partners.” Such a broad definition, including the fact that the CF included cyber incidents related to business partners, leaves little left untouched by the Guidance with regard to cyber events. For so many companies to be required to make a proactive assessment of the risk and potential consequences of some unknown type of cyber incident by unknown third parties will be a significant challenge.

What does the Guidance provide with respect to disclosures?

The Guidance provides a general overview of “specific disclosure obligations that may require a discussion of cybersecurity risks and cyber incidents,” and examples of when disclosure may be appropriate or required under existing SEC rules.

A. Risk Factors

According to the Guidance, “[r]egistrants 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.” Further, in determining whether risk factor disclosure is *required*, the Staff “expects registrants to evaluate their cybersecurity risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents. As part of this evaluation, registrants should consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption. In evaluating whether risk factor disclosure should be provided, registrants should also consider the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware.”

Under the Guidance, it is not just known cyber incidents that require attention: “[A] registrant may need to disclose known or threatened cyber incidents to place the discussion of cybersecurity risks in context. For example, if a registrant experienced a material cyber attack in which malware was embedded in its systems and customer data was compromised, it likely would not be sufficient for the registrant to disclose that there is a risk that such an attack may occur. Instead, as part of a broader discussion of malware or other similar attacks that pose a particular risk, the registrant should consider the need to discuss the occurrence of the specific attack and its known and potential costs and other consequences.”

Especially challenging is the suggestion that any assessment of material cybersecurity risks should address the potential costs and consequences of a possible breach. The Guidance also specifically highlights risks posed by outsourced functions. Issuers should consider whether their service providers are contractually obligated to provide the insight into their security protocols, controls and incident responses necessary to formulate appropriate disclosures. Note also that a description of relevant insurance coverage may also be needed. Whether there is coverage and the scope of that coverage may be difficult to address.

Importantly, the Guidance provides that any disclosure should be tailored to the company’s “particular circumstances and avoid generic ‘boilerplate’ disclosure.”

B. MD&A

The Guidance also addresses a registrant's approach to cyber risks and incidents in the context of Item 303 and the MD&A discussion. In short, the Guidance states that the registrant "should address cybersecurity risks and cyber incidents in their MD&A if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition."

C. Description of Business

In addition, the Guidance addresses disclosure under Item 101. Pursuant to the Guidance, "[i]f one or more cyber incidents materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions, the registrant should provide disclosure in the registrant's 'Description of Business.' "

D. Legal Proceedings

The Guidance also speaks to Item 103: "If a material pending legal proceeding to which a registrant or any of its subsidiaries is a party involves a cyber incident, the registrant may need to disclose information regarding this litigation in its 'Legal Proceedings' disclosure."

E. Financial Statement Disclosures

The Guidance notes that "cybersecurity risks and cyber incidents may have a broad impact on a registrant's financial statements, depending on the nature and severity of the potential or actual incident." In short, the Guidance provides that before a cyber incident, "registrants may incur substantial costs to prevent cyber incidents. Accounting for the capitalization of these costs is addressed by Accounting Standards Codification (ASC) 350-40, Internal-Use Software, to the extent that such costs are related to internal use software." In addition, during and after a cyber incident "[r]egistrants may seek to mitigate damages from a cyber incident by providing customers with incentives to maintain the business relationship." Moreover, cyber incidents may result in losses from asserted and unasserted claims and diminished future cash flows. The Guidance recognizes that registrants may not immediately know the impact of a cyber incident and may be required to develop estimates to account for the various financial implications and that any such assessments require reassessment.

F. Disclosure Controls and Procedures

According to the Guidance, registrants are "required to disclose conclusions on the effectiveness of disclosure controls and procedures. To the extent cyber incidents pose a risk to a registrant's ability to record, process, summarize, and report information that is required to be disclosed in Commission filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective." This requirement may present a challenge to registrants when, for example, the registrant is subject to an ongoing attack and the extent of the compromise remains under investigation.

What should a company do?

Notwithstanding the nonbinding nature of the Guidance, we strongly recommend that companies take affirmative steps to address the Guidance with respect to *both* cybersecurity matters and cyber incidents. It is clear from the Guidance that the SEC is taking a proactive approach to disclosure of cybersecurity risks, both before and after a cyber incident. Disclosure and cybersecurity business teams and counsel should coordinate carefully on any company response to the Guidance.

Cybersecurity is an increasingly critical issue. As a result, issuance of the Guidance may, as a general matter, be an appropriate step for the SEC to take. At the same time, however, there is reason for concern about the challenges companies face when disclosing the risks associated with cybersecurity matters and cyber incidents. We hope those in charge of enforcement and members of the judiciary consider these challenges and give full recognition to the perils of 20/20 hindsight.

Contacts

Allen C. Goolsby
agoolsby@hunton.com

David C. Lashway
dlashway@hunton.com

Randall S. Parks
rparks@hunton.com

Lisa J. Sotto
lsotto@hunton.com

John W. Woods, Jr.
jwoods@hunton.com

© 2011 Hunton & Williams LLP. Attorney advertising materials. These materials have been prepared for informational purposes only and are not legal advice. This information is not intended to create an attorney-client or similar relationship. Please do not send us confidential information. Past successes cannot be an assurance of future success. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials.