Hogan Lovells

SEC Update

October 25, 2011

Print

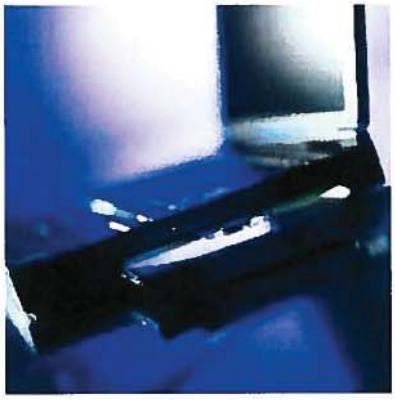
See note below about Hogan Lovells

SEC Issues Guidance on Disclosure of Cybersecurity Risks and Cyber Incidents

On October 13, the SEC's Division of Corporation Finance issued a "disclosure guidance" regarding the obligations of public companies to disclose cybersecurity risks and cyber incidents. The guidance follows a communication in May 2011 from five members of the Senate Committee on Commerce, Science and Transportation to SEC Chair Mary Schapiro asking the SEC to issue guidance regarding disclosure of information security risk, including material network breaches. The SEC staff responded to this request by issuing the second installment of its newest form of written guidance, entitled "CF Disclosure Guidance: Topic No. 2, Cybersecurity," which presents the views of the Division of Corporation Finance, but is not a rule, regulation or statement of the Commission. The staff advises companies to review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity matters in light of their specific facts and circumstances and, if appropriate in light of the guidance, to disclose the risks and incidents to investors. The seven-page guidance can be found at www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

Overview

The staff's guidance does not modify or add to any of the SEC's current disclosure requirements. Instead, the staff discusses how companies should describe cybersecurity matters and their potential impacts within the existing disclosure framework, and in particular under the Regulation S-K items that relate to risk factors, management's discussion and analysis, description of the business, legal proceedings, and disclosure controls, and procedures. The staff also highlights the manner in which such matters may affect financial statement disclosure. In identifying the various ways in which companies may need to disclose cybersecurity risks and cyber incidents, the staff indicates that it designed the guidance "to be consistent with the relevant disclosure considerations that arise in connection with any business risk." The recent focus by legislators and regulators on disclosure related to this particular business risk seems to stem from a perception that as dependence on information technology has increased, so too have the risks to



Contacts

Peter J. Romeo (Co-Editor)
peter.romeo@hoganlovells.com
+1 202 637 5805

Richard J. Parrino (Co-Editor)
richard.parrino@hoganlovells.com
+1 202 637 5530

Kevin K. Greenslade
kevin.greenslade@hoganlovells.com
+1 703 610 6189

Christopher Wolf
christopher.wolf@hoganlovells.com
+1 202 637 8834

Visit us at
www.hoganlovells.com

public companies associated with cybersecurity and cyber incidents.

The guidance describes "cybersecurity" as "the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access." The staff points out that the potential material costs and other negative consequences to a public company that is unable to protect itself from a cyber attack by a third party might include:

- Remediation costs incurred to satisfy liability for stolen assets or information, to repair system damage, or to offer incentives to customers or other business partners to maintain business relationships after an attack;
- Increased cybersecurity protection costs;
- Lost revenues stemming from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- Litigation; and
- Reputational damage adversely affecting customer or investor confidence.

Disclosure of cybersecurity risks and cyber incidents under existing framework

The new guidance notes that, although no existing SEC disclosure requirement expressly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents, as discussed in more detail below. In addition, the SEC staff reminds public companies that material information regarding cybersecurity matters is required under SEC disclosure rules to be included in SEC filings when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading. The staff also cautions that the same principle underlies the antifraud provisions of the federal securities laws, which apply to statements both in SEC filings and in other communications.

Many companies undoubtedly will struggle to determine the appropriate level of detail to include in their cybersecurity disclosures. The guidance acknowledges the challenges a company can face in crafting meaningful disclosure on this subject without jeopardizing its information security. The staff says that it is mindful of concerns that "detailed disclosures could compromise cybersecurity efforts – for example, by providing a 'roadmap' for those who seek to infiltrate a registrant's security network – and we emphasize that disclosures of that nature are not required under the federal securities laws." But the staff nevertheless admonishes companies, in accordance with existing Regulation S-K requirements for risk factor disclosures, to present individualized disclosures on cybersecurity risks, rather than generic risks that could apply to any issuer or any offering. In light of this tension, it is instructive to consider the staff's views on how specific issues of cybersecurity may be addressed under various items of Regulation S-K.

Risk factors. Item 503(c) of Regulation S-K requires a company to discuss the most significant factors that make an investment in its securities speculative or risky. In evaluating whether cybersecurity risks are among such factors, the staff advises companies to assess their risks in the following manner:

> [W]e expect registrants to ... 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.

While reiterating that disclosures need not and should not compromise a company's security, the staff

emphasizes that appropriate disclosures must adequately describe the nature of material risks and specify how the risks affect the company. To the extent material in light of the company's particular facts and circumstances, the disclosures may address the following matters, among others:

- The aspects of the company's business or operations that give rise to material cybersecurity risks and the potential costs and other consequences of the risks;
- Any outsourced functions that have material cybersecurity risks, and how the company addresses those risks;
- Cyber incidents actually experienced by the company that are material individually or in the aggregate, including a description of the costs and other consequences of the incidents;
- Risks involving cyber incidents that may remain undetected for an extended period; and
- Relevant insurance coverage maintained by the company.

MD&A. Item 303 of Regulation S-K generally requires a company's periodic reports and registration statements to contain a management's discussion and analysis of financial condition and results of operations (MD&A). The staff advises that companies should address cybersecurity risks and cyber incidents in MD&A if the costs or other consequences stemming from one or more *known* cyber incidents, or the risks of *potential* cyber 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 indicative of future operating results or financial condition. By way of illustration, the staff advises that if it is reasonably likely that a cyber attack resulting in the theft of material intellectual property will lead to reduced revenues, or an increase in cybersecurity protection or litigation costs, the company should discuss these possible outcomes, including the amount and duration of the expected costs if they are material.

Description of business. Item 101 of Regulation S-K requires a narrative description of the business of a company and its subsidiaries. The staff advises that, if one or more cyber incidents materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions, the business description should include appropriate disclosure about those incidents. In evaluating the need for disclosure under Item 101, companies should consider the impact on each reportable segment. For example, if a company has a new product in development and learns of a cyber incident that could materially impair the product's future viability, the incident and the potential effect should be discussed to the extent material.

Legal proceedings. Item 103 of Regulation S-K generally requires disclosure of any material pending legal proceedings to which a company is a party or to which its property is subject, as well as any similar actions known to be contemplated by governmental authorities. The guidance notes that if such a proceeding involves a cyber incident (for example, the theft of a significant amount of customer information), the company should disclose any information pertaining to the proceeding called for by Item 103.

Disclosure controls and procedures. Item 307 of Regulation S-K requires companies to disclose on a quarterly basis conclusions on the effectiveness of the company's disclosure controls and procedures. The staff urges companies to consider whether there are any deficiencies in their disclosure controls and procedures related to the risks posed by cyber incidents, such as a cyber incident affecting information systems, that would render the controls and procedures ineffective.

Considerations for financial statement disclosure

The SEC staff highlights several ways in which cybersecurity risks and cyber incidents may affect a company's financial statements, whether before an incident or during and after an incident. Before a cyber incident, companies may need to account for the capitalization of costs incurred in the prevention of cyber incidents, and should rely on the applicable accounting guidance in that regard. During and after an incident, financial statements may be affected in a number of ways, including the following identified by the staff:

- To the extent that a company seeks to mitigate damages from a cyber incident by providing customers with incentives to maintain the business relationship, it should consider ASC 605-50, *Customer Payments and Incentives*, to ensure appropriate recognition, measurement and classification of the incentives.

- To the extent that a company may suffer losses from asserted and unasserted claims relating to a cyber incident (for example, related to warranties, contract breaches, product recall and replacement, or indemnification of counterparty losses), it should consider ASC 450-20, *Loss Contingencies*, to determine when to recognize a liability.

- To the extent that a cyber incident may result in diminished future cash flows, a company should consider the need to record an impairment of certain assets, including goodwill, customer-related intangible assets, trademarks, patents, capitalized software or other long-lived assets associated with hardware or software, and inventory.

- To the extent that a cyber incident is discovered after the balance sheet date but before the issuance of the financial statements, a company should consider whether disclosure of a recognized or nonrecognized subsequent event is necessary.

Looking ahead

The staff's guidance should cause public companies to focus more intensively on assessing what disclosure, if any, they should provide concerning the cybersecurity risks they face and their history of, and exposure to, cyber incidents. The assessments are likely to be challenging for many companies, which may be well served by adding information technology and data security personnel to their disclosure review team.

The need for timely and thorough disclosure will add significant pressure to the monitoring and evaluation exercise. Companies must be prepared, in the event of a cyber incident, to consider not only what disclosure may be needed in the next periodic report filed with the SEC, but also whether it might be necessary to file promptly a current report on Form 8-K, for instance to maintain the accuracy of public information in the context of a securities offering or for Regulation FD purposes. Planning for these contingencies should take account of the possibility that the staff's focus on cybersecurity disclosures may embolden plaintiffs suing companies that are subjected to cyber incidents to claim that the related cybersecurity risks were not properly or timely disclosed.

Webinar on October 31

The new guidance will be discussed in a webinar to be held on October 31 at 2:00 PM EST/11:00 AM PST featuring senior lawyers in the Hogan Lovells Capital Markets and Privacy and Information Management practices, as well as a managing director of Stroz Friedberg LLC, a technology firm assisting clients with digital risks. Please click here to RSVP.

outcomes for other clients.