

SEC FLASH REPORT

SEC Staff Provides Guidance on Public Companies' Disclosure Obligations Relating to Cybersecurity Risks and Cyber Incidents

October 17, 2011

Last week, the staff of the Securities and Exchange Commission (SEC) issued guidance on an issuer's disclosures regarding cybersecurity risks and cyber incidents. This CF Disclosure Guidance represents the views of the Division of Corporation Finance. While not a rule, regulation or official statement of the Commission and while the Commission itself has neither approved nor disapproved the content of this guidance, issuers choosing to ignore advice from the staff of the Division of Corporation Finance and failing to assess and disclose material cybersecurity risks do so at the risk of filing delays and other regulatory action as well as increased exposure to the plaintiff bar.

The information in this disclosure guidance is intended to assist issuers in preparing disclosures required in registration statements under the Securities Act of 1933 and periodic reports under the Securities Exchange Act of 1934. In order to maintain the accuracy and completeness of information in effective shelf registration statements, issuers 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 should any occur.

In issuing this guidance, the SEC staff noted that they are mindful of the risk of providing a road map to cybercriminals who seek to infiltrate an issuer's network security. No one wants that to happen. Therefore, the staff noted that detailed disclosures that could compromise cybersecurity efforts are not required under the federal securities laws.

The guidance is available at <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm> on the SEC website. It is discussed further below.

Overview

Cybersecurity is the measures taken – in the form of technologies, processes and practices – to protect networks, systems, computers, applications and data from attack, damage or unauthorized access. While no specific disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, these risks and their potential impact on a business are hard to ignore if significant. There are a number of disclosure requirements that may impose an obligation on issuers to disclose such risks and incidents even though these requirements do not explicitly refer to cybersecurity risks. As issuers migrate toward increasing dependence on digital technologies to conduct their operations, the risks associated with cybersecurity increase, resulting in greater exposure of the company's systems and data, as well as of the data of customers and business partners, to more frequent and severe cyber incidents. These incidents can arise from either deliberate attacks or unintentional events.

In issuing its disclosure guidance, the SEC staff noted that they have observed an increased level of attention focused on cyber attacks. To that end, the guidance summarizes potential negative consequences and substantial costs that an issuer may incur as a result of a successful cyber attack. These consequences and costs include, but are not limited to, gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. The disclosure guidance further discusses these impacts, setting the stage for disclosure of these risks.

The question arises as to how cybersecurity risks and their related impact on an issuer's operations should be described within the framework of disclosure obligations imposed by the federal securities laws. In this context, the SEC staff concluded that it would be beneficial to provide guidance that assists issuers in assessing what, if any, disclosures should be provided about cybersecurity matters in light of each issuer's specific facts and circumstances.

The SEC staff noted in the disclosure guidance that the federal securities laws, in part, are designed to elicit disclosure of timely, comprehensive and accurate information about risks and events that a reasonable investor would consider important to an investment decision.

- As to when cybersecurity risks should be disclosed in SEC filings, the guidance states that issuers are required to conduct a risk assessment and evaluate the adequacy of preventive actions taken to reduce cybersecurity risks in the context of both the identified security risks and the industry in which they operate. The results of a risk assessment should determine whether there is material information regarding cybersecurity risks and cyber incidents that is required to be disclosed in order to make other required disclosures, in light of the circumstances under which they are made, not misleading. Accordingly, as with other operational and financial risks, issuers should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents in light of an ongoing assessment of risk. *The SEC staff's reference to consideration of the adequacy of preventive actions would appear to create a presumption that management would not need to disclose anything if the risk assessment were to determine that such mitigating actions reduced cybersecurity risks to an acceptable level. However, management would be advised to consult with legal counsel before reaching this conclusion in the face of significant cybersecurity risks.*
- As to what disclosure is necessary, the guidance provides examples of the appropriate disclosures. The disclosure guidance states that, depending on the circumstances and the company's particular situation, public filings may be impacted in several areas, e.g., the summary of risk factors, the management's discussion and analysis of financial condition and results of operation (MD&A), the descriptions of business and legal proceedings and, of course, financial statement disclosures.

The following sections provide a discussion of specific areas of disclosure obligations that may require a discussion of cybersecurity risks and cyber incidents.

Risk Factors

Item 503(c) of Regulation S-K requires issuers to 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. Consistent with the Item 503(c) requirements, issuers should not present risks that could apply to any issuer or any offering and should avoid generic "boilerplate" risk factor disclosure.

In determining whether risk factor disclosure is required for cybersecurity risks and cyber incidents, the SEC staff expects issuers 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, issuers 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, issuers should also consider the adequacy of preventive actions taken to reduce cybersecurity risks to an acceptable level in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware.

Cybersecurity risk disclosure provided must adequately describe the nature of the material risks and specify how each risk affects the issuer. Depending on the issuer's particular facts and circumstances, and to the extent material, the SEC staff provided the following examples of appropriate disclosures:

- Discussion of aspects of the issuer's business or operations that give rise to material cybersecurity risks and the potential costs and consequences
- To the extent the issuer outsources functions that have material cybersecurity risks, description of those functions and how the issuer addresses those risks
- Description of cyber incidents experienced by the issuer that are individually, or in the aggregate, material, including a description of the costs and other consequences
- Risks related to cyber incidents that may remain undetected for an extended period
- Description of relevant insurance coverage

The SEC staff notes that an issuer may need to disclose known or threatened cyber incidents to place the discussion of cybersecurity risks in context. For example, if an issuer 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 issuer 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 issuer may need to discuss the occurrence of the specific attack and its known and potential costs and other consequences.

While issuers should provide disclosure tailored to their particular circumstances and avoid generic "boilerplate" disclosure, the SEC staff reiterates that the federal securities laws do not require disclosure that itself would compromise an issuer's cybersecurity. Instead, issuers should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular issuer in a manner that would not have that consequence. *It is left to the discretion of management to decide the extent of detail that best meets the issuer's obligations under the securities laws while not compromising its cybersecurity.*

Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A)

According to the SEC staff, issuers 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 issuer'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." The SEC staff notes that an example of an event triggering such disclosures would be the theft of material intellectual property in a cyber attack. For example, if material intellectual property is stolen in an attack and the effects of the theft are reasonably likely to be material, the issuer should describe the stolen property and the effect of the attack on its

results of operations, liquidity and financial condition, and note whether the attack would cause reported financial information not to be indicative of future operating results or financial condition. If it is reasonably likely that the attack will lead to reduced revenues and/or an increase in cybersecurity protection costs, including those related to litigation, the issuer should discuss these possible outcomes, including the amount and duration of the expected costs, if material. Alternatively, if the attack did not result in the loss of intellectual property, but it prompted the issuer to materially increase its cybersecurity protection expenditures, the issuer should disclose those increased expenditures.

Legal Proceedings

Item 103 of Regulation S-K (“Legal Proceedings”) requires a brief description of “material pending legal proceedings, other than routine litigation incidental to the business.” If a material pending legal proceeding to which an issuer or any of its subsidiaries is a party involves a cyber incident, the issuer may need to disclose information regarding this litigation in its “Legal Proceedings” disclosure. For example, if a significant amount of customer information is stolen as a result of a cyber incident and the liability that could be incurred by the company is material, any litigation arising is likely to be material. In such instances, the SEC staff states that the issuer disclose the name of the court in which the proceedings are pending, the date instituted, the principal parties thereto, a description of the factual basis alleged to underlie the litigation, and the relief sought.

Financial Statement Disclosures

Cybersecurity risks and cyber incidents may have a broad impact on an issuer’s financial statements, depending on the nature and severity of the potential or actual incident. The disclosure guidance references various accounting principles that may be implicated in the event of a cyber incident, including loss contingencies, cash flow diminution, and customer payments and incentives that may result from an issuer seeking to mitigate damages.

Following is guidance provided by the SEC staff:

- **Prior to a Cyber Incident** – Issuers 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.
- **During and After a Cyber Incident** – Issuers may seek to mitigate damages from a cyber incident by providing customers with incentives to maintain the business relationship. Issuers should consider ASC 605-50, *Customer Payments and Incentives*, to ensure appropriate recognition, measurement and classification of these incentives.

Cyber incidents may result in losses from asserted and unasserted claims, including those related to warranties, breach of contract, product recall and replacement, and indemnification of counterparty losses from their remediation efforts. Issuers should refer to ASC 450-20, *Loss Contingencies*, to determine when to recognize a liability if those losses are probable and reasonably estimable. In addition, issuers must provide certain disclosures of losses that are at least reasonably possible.

Cyber incidents may also result in diminished future cash flows, thereby requiring consideration of 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. Issuers may not immediately know the impact of a cyber incident and may be required to develop estimates to account for the various financial implications. Issuers should subsequently reassess the assumptions that

underlie the estimates they made in preparing the financial statements. In accordance with FASB ASC 275-10, *Risks and Uncertainties*, an issuer must explain any risk or uncertainty of a reasonably possible change in its estimates in the near-term that would be material to the financial statements. Examples of estimates that may be affected by cyber incidents include estimates of warranty liability, allowances for product returns, capitalized software costs, inventory, litigation and deferred revenue.

To the extent a cyber incident is discovered after the balance sheet date but before the issuance of financial statements, issuers should consider whether disclosure of a recognized or non-recognized subsequent event is necessary. If the incident constitutes a material non-recognized subsequent event, the financial statements should disclose the nature of the incident and an estimate of its financial effect, or make a statement that such an estimate cannot be made.

Description of Business

Item 101 of Regulation S-K (“Description of the Business”) requires a description of the company’s business. If one or more cyber incidents materially affect an issuer’s products, services, relationships with customers or suppliers, or competitive conditions, the issuer should provide disclosure in the issuer’s “Description of Business” section. In determining whether to include disclosure, issuers should consider the impact on each of their reportable segments. As an example, if an issuer has a new product in development and learns of a cyber incident that could materially impair its future viability, the issuer should discuss the incident and the potential impact to the extent material. If incidents have already impacted, or may materially impact, the issuer’s business or if there are pending material legal proceedings, full disclosure should be made.

Disclosure Controls and Procedures

Item 307 of Regulation S-K (“Disclosure Controls and Procedures”) requires disclosure of the company’s conclusions regarding the effectiveness of its disclosure controls and procedures. To the extent cyber incidents pose a risk to an issuer’s ability to record, process, summarize and report information that is required to be disclosed in SEC filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective. For example, if it is reasonably possible that information would not be recorded properly due to a cyber incident affecting an issuer’s information systems, an issuer must consider whether this condition has impaired the effectiveness of its disclosure controls and procedures. A conclusion that this effectiveness has been impaired would affect the issuer’s executive certification under Section 302 of Sarbanes-Oxley.

Summary

The SEC staff’s guidance is likely to result in public companies engaging in a substantial and detailed assessment of their cybersecurity risks to determine if public disclosure is required. It may also lead to a trend of the plaintiff bar suing corporations following a data security breach, alleging that the risks of such a breach were not properly assessed or disclosed. This adds another layer of complexity to an already complex matter.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE® 1000 and Global 500 companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half International Inc. (NYSE: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.