Print This Article

<< Return to SEC's Corp Fin Staff Attacks Cyber-Security Disclosure

SEC's Corp Fin Staff Attacks Cyber-Security Disclosure

Reese Darragh
October 25 2011

The Securities and Exchange Commission's latest burst of staff guidance—again delivered in the agency's new, non-binding format of “CF Disclosure”—takes aim at the tricky realm of disclosing cyber-security risks.

The seven-page document, published by staff in the Division of Corporation Finance (hence the “CF”) outlines items companies should consider when identifying specific business risks caused by cyber-security incidents. Among them: how those costs might affect the balance sheet; the correlation of those risks to the company's business model; possible legal proceedings; and how to make appropriate financial statement disclosure to reflect the effect of a cyber-attack.

What's more, the SEC wants companies to conduct a self-assessment of their ability to file accurate and timely disclosures to the Commission in the event of an attack.

The guidance says that while no existing disclosure requirement explicitly refers to cyber-security risks or attacks, a number of disclosure requirements can impose an obligation on companies to disclose the information. “In addition, material information regarding cyber-security risks and cyber-incidents is required to be disclosed when necessary to make other required disclosures, in light of the circumstances under which they are made, not misleading,” the SEC staff said in a release with the guidance.


Shirodkar

In other words, says Sanjay Shirodkar, counsel at law firm DLA Piper, the SEC staff considers cyber-security disclosure important, “and it is likely that they will be issuing more comments regarding the matters in the guidance.” He said the guidance is intended to highlight the SEC's expectation that public companies include cyber-security matters in their business risk assessments, such as the Management Discussion & Analysis in the Form 10-K.

The guidance is divided into five summary segments, each describing different disclosure obligations relating to cyber-security risks and incidents. In the first section of risk factors disclosures, companies are asked to evaluate the frequency of cyber incidents occurring in their businesses, the quantitative and qualitative level of those risks (including potential costs resulting from these incidents), and negative consequences to their operations.

The guidance stresses that the risk disclosures must be consistent with requirements in Regulation S-K, which says companies must provide information to describe the nature of the material risks adequately and to specify how each risk affects their businesses.

The second segment advises management to discuss cyber-incidents that have a significant effect on their businesses in the MD&A. Management should tell investors how known or potential incidents can significantly affect the companies' current and future financial performances. Companies should highlight any increased

expenditures that might be necessary to implement higher levels of security to protect their cyber-infrastructure, and the cost of any litigation.

"It is likely that [SEC staff] will be issuing more comments regarding the matters in the guidance."

—Sanjay Shirodkar,
Counsel,
DLA Piper

Companies should also take note of the possible requirement to include cyber-incidents in the business description section of their filings, if such incidents have a significant consequence to their products, services, business relationships with clients and suppliers, or their market competitiveness. Information on any legal proceedings related to a data breach must also be included.

When submitting financial statements, companies are advised to incorporate relevant cost increases and revenue shortfalls if operations are affected by cyber-incidents. The SEC staff asked that companies disclose their prevention costs in financial statements *prior* to any cyber-attack. In the period during and after an incident, companies should incorporate the costs to mitigate damages, losses, and drops in cash flows as well.

The last segment of the guidance describes the requirement for companies to self-assess the effectiveness of their disclosure controls and procedures in the event of a cyber-attack. Companies are asked to consider if their information systems have any weaknesses that might potentially undercut their ability to capture the information to be disclosed to the Commission. Businesses are advised to grade their systems, whether effective or ineffective, and include the assessment in their periodic filings.

FINANCIAL STATEMENT DISCLOSURES

The following excerpt is from the SEC Corp Fin guidance on cyber-security:

Cyber-security 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.

Prior to 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.

During and After a Cyber Incident

Registrants may seek to mitigate damages from a cyber incident by providing customers with incentives to maintain the business relationship. Registrants 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. Registrants 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, registrants 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. 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. Registrants should subsequently reassess the assumptions that underlie the estimates made in preparing the financial statements. A registrant 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, registrants 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 a statement that such an estimate cannot be made. **Disclosure Controls and Procedures**

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. For example, if it is reasonably possible that information would not be recorded properly due to a cyber incident affecting a registrant's information systems, a registrant may conclude that its disclosure controls and procedures are ineffective.

Source: Corp Fin's Staff Guidance on Cyber-Security.

The SEC staff also reminded companies that while they should provide disclosure specific to circumstances and (as always) avoid generic boilerplate disclosure, federal securities law does not require details that would harm a company's cyber-security infrastructure. “Instead, 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,” the guidance says.

Disclosure in Practice

Lawyers agree that while the guidance spelled out the framework of how companies should disclose statements relating to cyber-security issues, the methods prescribed aren't terribly well defined.


Dunne

“The SEC staff in this guidance says, ‘We do not want you to disclose the roadmap of your system such that cyber-security would be compromised, but we want you to avoid generic descriptions while adequately describing the nature of the risk.' It's hard to make sense of what they want,” says Julie Dunne, associate at law firm Wiley Rein.

But, she adds, the lack of specific disclosure requirements in the guidance may give companies flexibility in assessing and disclosing cyber-security-related information. She says companies must do their own individual risk analysis since cyber-risk profiles will be very fact-specific.


Zick

Colin Zick, a partner at law firm Foley Hoag, says the guidance is too general and that companies will have to think hard when assessing what information to disclose. “There are a lot of cyber-incidents, and there are lots of ways how these will affect your business,” he says. When companies are contemplating the definition of cyber-incidents, they should think expansively, he adds. “Think of data breach, data loss, and denial of service on your Websites when an attack occurs. The [SEC staff] wants you to do this risk assessment so you will understand what this is about,” he said.

Others say the guidance is nothing new.

Shirodkar quoted some prior examples of similar interpretive guidance such as those related to the Y2K bug and the interpretive release on climate change the SEC issued last year. “The general analysis that a public company must undertake in evaluating business risks has not changed,” he says; the only difference is that the SEC cannot tell companies which incidents are material to them and which aren't. Companies will have to assess facts and circumstances specific to the nature of their businesses in order to determine what information to disclose, he says.


Badway

Ernest Badway, a partner at law firm Fox Rothschild, agrees. The SEC staff wants companies to adopt the same thought process they gave to preparing disclosures on past hot topics. In this instance, he says, companies will have to disclose policies and procedures in place that relate to data protection. And even if a company has outsourced its data storage functions to third-party vendors, they're still responsible for these disclosures, he says.

Badway suggests a three-prong strategy to comply with the disclosure requirements. First, determine the "inventory" of your data and infrastructure, and identify what type of information needs protection. Next, develop procedures and policies based on that inventory, allocating more resources to data that requires additional protection, such as patent information and proprietary data. Finally, prepare corrective measures that can be taken after an incident. "Have procedures in place to identify these incidents and steps to take after the attack," he says.