White Paper

pillsbury

Global Sourcing

November 17, 2011

Accounting for Cybersecurity: SEC Guidance on Disclosures to Investors and Regulators

by John L. Nicholson

On October 13, the Securities and Exchange Commission (SEC) Division of Corporation Finance released CF Disclosure Guidance: Topic No. 2 - Cybersecurity (the "Guidance"), which is intended to instruct companies on whether and how to disclose the impact of the risk and cost of cybersecurity incidents (both malicious and accidental) on a company.

This represents a reminder that companies should think about cybersecurity and data breach incidents when deciding how to fulfill their obligations under the SEC's existing disclosure requirements. Up to this point, the market's focus has been on how U.S. law requires disclosure of data breaches affecting personal information of specific types. Other security incidents only became public knowledge because of unofficial disclosures or because of their effect (e.g., a denial of service attack). Now, the SEC has made it clear that the risks associated with cyber incidents, the costs of mitigating those risks, and the consequences of a cyber incident may rise to the level of materiality that would require disclosure to investors and regulatory authorities.

Although the Guidance is not, in itself, a rule or regulation, companies who ignore such guidance may do so at their peril.

From the Guidance:

> "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**. Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents. In addition, **material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading.** Therefore, as with other operational and financial risks, registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents." [Emphasis added]

Evaluation of a company's own cybersecurity profile is hard enough, but it's made even more difficult in a world where a significant portion of a company's services are outsourced and cloud-based.

Although the SEC's language focuses on cyber attacks, many of those same consequences would apply to an accidental incident. Given the potential adverse consequences of a cyber incident, the Guidance states, "as with other operational and financial risks, registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents."

The remainder of the Guidance focuses on how companies should disclose and discuss cyber incidents in the context of various reporting obligations. In that area, the SEC has engaged offered up a somewhat ambiguous standard — on one hand, the Guidance appears to allow for a lack of specific details in order to avoid compromising a company's security, but on the other hand, the SEC cautions companies not to use any sort of generic "boilerplate" language in its disclosure. The tightrope offered up by the Guidance states:

> "While [companies] should provide disclosure tailored to their particular circumstances and avoid generic "boilerplate" disclosure, we reiterate that the federal securities laws do not require disclosure that itself would compromise a [company's] cybersecurity. Instead, [companies] should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular [company] in a manner that would not have that consequence."

Risk

To determine whether your company is required to disclose a particular cyber-related risk factor in accordance with the Regulation S-K Item 503(c) requirements, the SEC has said that companies should evaluate their cybersecurity risks and take into account all available relevant information, including:

- prior cyber incidents and the severity and frequency of those incidents;
- the probability of cyber incidents occurring;
- threatened attacks of which they are aware, which could include things like the hacker group Anonymous' potential threats to attack Facebook;
- the quantitative and qualitative magnitude of those risks, including potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption;
- the adequacy of preventative actions taken to reduce cyber-related risks in the context of the industry in which they operate and risks to that security.

Tying these to the industry in which a company operates might also mean that a company needs to consider the recent U.S. Department of Homeland Security report that raises the possibility that members of Anonymous are actively looking for ways to attack critical infrastructure. At the same time, however, the Guidance states that risk disclosure must adequately describe the nature of the material risks and how each risk affects the company. According to the SEC, companies should not present risks that could apply to any company and should avoid generic risk factor disclosure.

Depending on your particular facts and circumstances, and to the extent material, appropriate disclosures may include:

- Discussion of aspects of your business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- If your company outsources functions that have material cybersecurity risks, description of those functions and how you address those risks;
- Description of cyber incidents your company has experienced 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; and
- Description of relevant insurance coverage.

According to the SEC, a company might have to disclose known or threatened cyber incidents to place the discussion of cybersecurity risks in appropriate context. The SEC provides the following example, "if a [company] 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 may need to discuss the occurrence of the specific attack and its known and potential costs and other consequences." In this context, if predictions from this Information Week article regarding the malware discovered in 2010 on the NASDAQ Director's Desk platform are correct, it will be interesting to see how companies might disclose the risks associated with that cyber attack.

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

The next section of the Guidance discusses the way that companies should address cybersecurity risks and cyber incidents under the reporting rules associated with Management's Discussion and Analysis of Financial Condition and Results of Operations ("MD&A") under Item 303 of Regulation S-K and Form 20-F, Item 5.

According to the SEC, the standard for discussion of cyber incidents in a company's MD&A is the same as for non-cyber events. Thus, if the costs or other consequences associated with a cyber incident, or the risk associated with potential incidents, represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on a company'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, then those costs, consequences or risks must be disclosed and discussed by the company.

For example, if intellectual property is stolen in a cyber attack, as was the case in the RSA attack, and the effects of the theft are reasonably likely to be material to the affected company, the Guidance suggests that the company should describe the stolen IP and the effect of the attack on its results of operations, liquidity, and financial condition and whether the attack would cause reported financial information not to be indicative of future operating results or financial condition. Since RSA is offering to replace all of the RSA SecureID tokens that could be affected by the information stolen in the RSA attack, at a potential cost of up to $52 million, that could rise to the level of a materiality. Similarly, if it

is reasonably likely that the hacking attack will lead to material reduction in revenues or a material increase in cybersecurity protection costs, including those related to litigation, the SEC wants the company to discuss these possible outcomes, including the amount and duration of the expected costs.

Alternatively, if a hacking attack or some other cyber incident did not result in harm to a company, but it prompted the company to materially increase its cybersecurity protection expenditures, the SEC wants the company to disclose those increased expenditures. However, the Guidance is careful to note that discussions of increased cybersecurity spending do not require disclosure of information that would make it easier to attack the company.

Other Disclosures

The Guidance goes through other disclosure requirements and provides examples of when a company might have to disclose information about a cyber incident.

If a cyber incident (or multiple incidents) materially affect a company's products, services, relationships with customers or suppliers, or competitive conditions, the company should provide disclosure in the company's "Description of Business" as required by Item 101 of Regulation S-K; and Form 20-F, Item 4.B. In determining whether to include disclosure, the SEC recommends that companies consider the impact on each of their reportable segments. For example, if a company has a new product in development and learns of a cyber incident that could materially impair the future viability of the product, the company should discuss the incident and the potential impact to the extent the impairment to the future of the product would be considered material. As in the previous section, the impact on RSA of the loss of intellectual property associated with the SecureID token could reach the level of materiality.

Similarly, if a company or any of its subsidiaries is a party to a litigation that involves a cyber incident, the company may need to disclose information regarding the litigation in its "Legal Proceedings" disclosure, just as it would any other litigation as required by Item 103 of Regulation S-K. For example, if a significant amount of customer information is stolen, as was the case in the Epsilon and RSA attacks, and the loss results in material litigation, the Guidance recommends that the affected company should disclose the name of the court in which the proceedings are pending, the date instituted, the principal parties, a description of the factual basis alleged to underlie the litigation, and the relief sought.

Finally, the Guidance notes that risk mitigation and cyber incidents could impact a company's financial statements, and the SEC has provided examples to help companies make sure costs are given the appropriate accounting treatment. The SEC notes, for example, that after a cyber incident companies might try to mitigate the business damage by providing customers with incentives to maintain the business relationship, which should be handled in accordance with FASB ASC 605-50, Customer Payments and Incentives. Similarly, 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, all of which should be handled in accordance with ASC 450-20, Loss Contingencies.

From a numerical accounting perspective, cyber incidents could also result in diminished future cash flows, requiring the affected company to consider the effect on certain assets including goodwill, customer-related intangible assets, trademarks, patents, capitalized software or other long-lived

assets associated with hardware or software, and inventory. According to the SEC, pursuant to FASB ASC 275-10, Risks and Uncertainties:

> "[Company] may not immediately know the impact of a cyber incident and may be required to develop estimates to account for the various financial implications. [Companies] should subsequently reassess the assumptions that underlie the estimates made in preparing the financial statements. A [company] 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."

If a cyber incident is discovered after a company's balance sheet date but before the company actually issues its financial statements, the SEC recommends that companies should consider whether disclosure of a recognized or nonrecognized subsequent event is necessary. If the cyber incident constitutes a material nonrecognized subsequent event pursuant to ASC 855-10, Subsequent Events, the company's financial statements should disclose the nature of the incident and an estimate of its financial effect, or they should include a statement that such an estimate cannot be made.

Disclosure Controls and Procedures

The Guidance is written at a fairly high level and does not prescribe any particular technologies or practices. However, there is an interesting statement at the end of the document:

> “To the extent cyber incidents pose a risk to a [company'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 [company's] information systems, a [company] may conclude that its disclosure controls and procedures are ineffective."

In other words, when determining whether a company’s disclosure controls and procedures are effective under Item 307 of Regulation S-K, management should consider how vulnerable those systems are to cyber incidents and whether the company can conclude in good faith that its disclosure controls and procedures are “effective.” It might be that disclosure controls and procedures should be considered “effective” only if they include a monitoring system that is protected from cyber attacks to recognize when an incident has occurred — which begs the question whether anything short of secure logging would be “effective.” On a local network, logging is relatively easy, but when we start incorporating multi-tenant cloud solutions into the environment, logging starts to get a lot more challenging. On a more general level, cloud providers have been reluctant to share information about their security efforts as well as any risks or failures that they don’t have to disclose.

Conclusion

The SEC has sent a message in no uncertain terms that it expects public companies to provide timely, accurate and complete-but-not-overly-disclosing information about cyber incidents and risks. While, from the SEC’s perspective, this new Guidance merely clarifies the existing requirement that public companies disclose “material” information to investors, these new guidelines impose significant obligations that such companies would almost certainly consider new. The impact of these new

requirements is magnified when combined with the whistleblower provisions in the Dodd-Frank Wall Street Reform and Consumer Protection Act. The Dodd-Frank Act offers a reward of 10-30% of any recovery over $1 million to informants who provide certain types of information leading to successful securities actions — notably including failure-to-disclose actions.

Companies now face the unenviable task of deciding what aspects of cyber incidents or risks are "material" and disclosing them, with the knowledge that the sophisticated and determined nature of today's cyber-attackers makes predicting the nature of an attack and its consequences incredibly difficult. The nature of the cyber threat is one that is constantly adapting and evolving. For example, should RSA have anticipated that an attacker would target information about their tokens and disclosed the risk that if someone did somehow compromise the algorithms embedded in the tokens, then RSA might have to spend $52 million replacing all of the tokens? Almost by definition, once such an event happens it could be considered a "risk" that should have been disclosed. And if a company does not disclose an event, their IT staff could collect a $100,000 - $300,000 bounty (or more) for information leading to a successful failure-to-disclose action.

It's considered axiomatic in the security community that it's not a question of whether a company will have a cyber incident, but, rather, when it will happen. Faced with these new disclosure obligations, companies should examine their own cybersecurity processes and procedures as well as those of their suppliers, look at their incident response plans, and examine their cyberinsurance coverage.

If you have any questions about the content of this white paper, please contact the Pillsbury attorney with whom you regularly work, or the author.

John L. Nicholson (bio)
Washington, DC
+1.202.663.8269
john.nicholson@pillsburylaw.com