JENNER&BLOCK

Corporate Advisory

October 17, 2011

Guidance on Cybersecurity Disclosure Obligations

by William L. Tolbert, Jr. and Elaine Wolff

In only the second topic published by the SEC's Division of Corporation Finance as "CF Disclosure Guidance: Topic 2," the Division provided guidance on the topic of disclosure obligations relating to cybersecurity risks and incidents ("Guidance").[1] Published on October 13, 2011, the Guidance follows an explosion of high profile cyber attacks at major corporations this year. In the much publicized attack on Sony in April, hackers stole the personal information of millions of registered users of Sony's PlayStation Network; in March, EMC Corporation's data security unit RSA, suffered a massive breach that resulted in the theft of data related to its SecurID tokens used by millions of private and government employees; and, in April several large financial institutions, including Citigroup and JP Morgan Chase, faced breaches of personal customer information when hackers penetrated a firm that handled their email communications as well as those of some of the largest companies in the United States.

Although there are no existing disclosure requirements that explicitly refer to cybersecurity risks and cyber incidents, the Guidance advises companies to consider whether the existing disclosure requirements in SEC filings impose a disclose obligation.

Summary

The Guidance seeks to balance the need for disclosure tailored to a company's particular experiences with cyber incidents with the need to avoid a "roadmap" for compromising a company's cybersecurity. Among the substantial costs and other negative consequences that should be considered for disclosure by companies that fall victim to successful cyber attacks are:

- Remediation costs related to liability for stolen assets or information, repairing system damage and incentives for customers or business partners to maintain business relationships following an attack;
- Increased cybersecurity protection costs that may include additional personnel and protection technologies, third party experts and training;
- Lost revenues from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- Litigation, and
- Reputational damage.

Is Disclosure Required?

The following sections of a company's public filings should be examined to determine whether disclosure about cybersecurity should be included.

Risk Factors

In determining whether cybersecurity risk factor disclosure is required, the Guidance advises companies to evaluate:

- previous cyber incidents,
- the severity and frequency of those incidents,
- the probability of cyber incidents occurring, and
- the quantitative and qualitative magnitude of the

risks, including the potential costs and other consequences resulting from the misappropriation of assets or sensitive information, corruption of data or operational disruption.

To the extent material, the Guidance indicates that the following disclosures may be appropriate:

- Those aspects of the company's business or operations that give rise to material cybersecurity risks and the potential costs and consequences,
- Outsourcing functions that pose material cybersecurity risks,
- Previous cyber incidents 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 extended periods, and
- Description of relevant insurance coverage.

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

Companies are advised to 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 the reported financial information not to be indicative of future operating results or financial condition. The Guidance cites the example of a company whose material intellectual property is stolen in a cyber attack. In that case, companies are counseled to describe the property that was stolen and the effect of the attack on its results of operations, liquidity and financial condition and whether an 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 suffered by the company will lead to reduced revenues, or an increase in cybersecurity protection costs, including those related to litigation, companies should discuss the possible outcomes, including the amount and duration of the expected costs, if material.

Description of Business

In determining whether to include disclosure, companies should consider whether one or more cyber incidents materially affect a company's products, services, relationships with customers or suppliers, or competitive conditions. Companies are directed to consider the impact on each of their reportable segments.

Legal Proceedings

If a material pending legal proceeding to which a registrant or any of its subsidiaries is a party involves a cyber incident, the registrant should 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

The Guidance points to the application of certain accounting standards that companies should consider. First, companies are counseled to consider the application of Accounting Standards Codification (ASC) 350-40, Internal-Use Software, that may require the capitalization of internal software costs incurred to prevent cyber incidents. Second, if a company provides incentives to maintain business relationships, it should consider ASC 605-50, Customer Payments and Incentives, to ensure appropriate recognition, measurement, and classification of these incentives. Third, companies should consider the application of ASC 450-20, Loss Contingencies, to determine when to recognize a liability and the required disclosures in connection with 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. Finally, companies that may suffer diminished future cash flows from cyber incidents should consider the 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 financial statements, companies should consider whether disclosure of a recognized or nonrecognized subsequent event is necessary. If the incident constitutes a material nonrecognized 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

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 its SEC filings, such as a cyber incident that affected a company's information systems, management should consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective.

ENDNOTES

1 CF Disclosure Guidance Topics: Topic No. 2 Cybersecurity http://www.sec.gov./divisions/corpfin/guidance/cfguidance-topic2.htm

For more information, please contact the following Jenner & Block attorney:

William L. Tolbert, Jr.
Partner
Tel: 202 639-6038
Email: wtolbert@jenner.com

Elaine Wolff
Partner
Tel: 202 637-6389
Email: ewolff@jenner.com