

Reproduced with permission from Privacy & Security Law Report, 10 PVLR 43, 10/31/2011. Copyright © 2011 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

Corporate Security

The Securities and Exchange Commission's Guidance On Cybersecurity and Cyber Incident Disclosure



BY MELISSA J. KRASNOW

Background

The U.S. Securities and Exchange Commission on occasion provides disclosure guidance on topics of interest to the business and investment communities. The SEC said recently that it has observed “an increased level of attention focused on cyberattacks.”¹

The rash of costly cyberattacks against companies like Epsilon and Sony, among others, gave the SEC cause to implement new cybersecurity disclosure requirements.²

¹ Division of Corporation Finance, U.S. Securities and Exchange Commission, *CF Disclosure Guidance: Topic No. 2* (Oct. 13, 2011), <http://www.sec.gov/divisions/corpfm/guidance/cfguidance-topic2.htm>.

² Bryce Baschuk, *New SEC Rules Require Companies to Disclose Cybersecurity Risks*, *Consumer Elec. Daily*, Oct. 17, 2011, available at 2011 WLNR 21479301.

Melissa J. Krasnow, a partner in the Corporate Group of Dorsey & Whitney LLP in Minneapolis, is a Certified Information Privacy Professional and serves on the International Association of Privacy Professionals Publication Advisory Board.

On Oct. 13 the SEC Division of Corporation Finance issued guidance for public companies regarding their disclosure obligations relating to cybersecurity (i.e., the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access) risks and cyber incidents in light of a public company's specific facts and circumstances. The guidance is not a rule, regulation or statement of the SEC.

The federal securities laws are designed in part for disclosure of timely, comprehensive and accurate information about risks and events that a reasonable investor would consider important to an investment decision. Although no disclosure requirement specifically refers to cybersecurity risks and cyber incidents, the guidance provides an overview of the following particular disclosure obligations that may require discussion of cybersecurity risks and cyber incidents: (1) risk factors, (2) management's discussion and analysis of financial condition and results of operations (MD&A), (3) description of business, (4) legal proceedings, (5) financial statement disclosure and (6) disclosure controls and procedures.

Risk factors

A public company should 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. A cybersecurity risk disclosure made by a company must adequately describe the nature of the material risks and specify how each risk affects the particular public company. Generic risk factor disclosure should be avoided.

A public company should evaluate its cybersecurity risks and consider previous cyber incidents (including severity and frequency), the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks (including the potential costs and other consequences). In evaluating whether risk factor disclosure should be provided, a public company also should consider the adequacy of preventative actions taken to reduce cybersecurity risks in the context

of the industry in which it operates and risks to that security (including threatened attacks it is not aware of).

Examples of disclosures may include: (1) discussion of aspects of the public company's business or operations that give rise to material cybersecurity risks and the potential costs and consequences; (2) to the extent the public company outsources functions that have material cybersecurity risks, a description of those functions and how the public company addresses those risks; (3) a description of cyber incidents experienced by the public company that are individually, or in the aggregate, material, including a description of the costs and other consequences; (4) risks related to cyber incidents that may remain undetected for an extended period and (5) a description of relevant insurance coverage.

The federal securities laws do not require disclosure that itself would compromise a public company's cybersecurity. Instead, a public company should provide sufficient disclosure to allow investors to appreciate the nature of the risks that it faces in a manner that would not have that consequence.

Management's discussion and analysis (MD&A) of financial condition and results of operations

A public company should address cybersecurity risks and cyber incidents in MD&A if the costs or other consequences associated with 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 its 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.

Description of business

In "Description of Business" a public company should provide disclosure if one or more cyber incidents materially affect its products, services, relationships with customers or suppliers or competitive conditions. In determining whether to provide disclosure, a public company should consider the impact on each of its reportable segments.

Legal proceedings

In "Legal Proceedings" a public company may need to provide disclosure if it or any subsidiary is a party to a material pending legal proceeding that involves a cyber incident. By way of example, if a significant amount of customer information is stolen, resulting in material litigation, the public 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.

Financial statement disclosure

Before a cyber incident, a public company may incur substantial costs to prevent cyber incidents. During and after a cyber incident, a public company may seek to mitigate damages by providing customers with incentives to maintain the business relationship. In addition, cyber incidents may result in losses from asserted and

unasserted claims, including warranties, breach of contract, product recall and replacement and indemnification of counterparty losses from their remediation efforts. If losses are probable and reasonably estimable, a public company should determine when to recognize a liability. Also, a public company must provide certain disclosures of losses that are at least reasonably possible.

Cyber incidents may also result in diminished future cash flows, 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. A public 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. A public company should subsequently reassess the assumptions that underlie the estimates made in preparing the financial statements. A public 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. 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, a public company should consider whether disclosure of a recognized or nonrecognized subsequent event is necessary. If the incident is 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

Where cyber incidents pose a risk to a public company'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. By way of example, if it is reasonably possible that information would not be recorded properly due to a cyber incident affecting a public company's information systems, a public company may conclude that its disclosure controls and procedures are ineffective.

Steps to take

Public companies should review the adequacy of their disclosure relating to cybersecurity risks and cyber incidents at present and on an ongoing basis. This review could implicate different areas, including legal, accounting, privacy, information technology, risk management/insurance and corporate communications. SEC disclosure considerations should be taken into account in terms of company preparation for cyber incidents and in applicable company policies, procedures and practices. Finally, a public company should review its insurance coverage relating to cybersecurity and cyber incidents, if any, in light of the guidance (e.g., risk factor disclosure).