



LOEB & LOEB adds Depth.

SEC Staff Issues Guidance Regarding Cybersecurity Risks And Incidents Disclosure

October 2011

The Staff of the Securities and Exchange Commission's Division of Corporate Finance has issued guidance regarding disclosure of risks of cyber-attacks and reporting of attacks that have occurred.

A reporting company that is dependent on digital technologies in conducting its business should consider disclosure of vulnerabilities to unintentional security breaches, as well as deliberate attacks, including by unauthorized access, denial of service, and social engineering. Deliberate attacks may be intended to steal assets, intellectual property, other sensitive information or to disrupt operations of the reporting company or its customers or others with whom the company has business relations. Resulting material costs may include:

- Recovery or replacement of lost assets and repair of damaged systems;
- Costs of improving cybersecurity;
- Reputational injury;
- Incentives given to maintain customer or other business relationships after an attack; or
- Litigation relating to and remediation of injuries suffered by third parties.

Obligations to disclose these risks and costs may arise under several reporting requirements.



LOEB & LOEB adds Depth.

Risk Factors

The guidance states that cybersecurity risks should be disclosed among a company's risk factors, if such risks "are among the most significant factors that make an investment in the company speculative or risky." Risk factor disclosure must adequately describe the nature of the risk and how it affects the company, but not present generic risks applicable to any company. However, a "roadmap" of the company's vulnerabilities is not required.

Management's Discussion and Analysis; Description of Business

Disclosure in a company's MD&A may be required, if the costs associated with known incidents or the risk of potential incidents constitute 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. Such effects may arise from loss of assets, systems remediation costs, liability to third parties, or impairment of reputation. Impacts on a company's products, services, business relationships, or competitive conditions may need to be disclosed in a company's description of its business.

Legal Proceedings

Significant litigation resulting from injuries to customers or vendors caused by a security breach may be reportable pursuant to legal proceedings disclosure requirements.

Financial Statement Disclosures

The Staff noted that Accounting Standards Codification 350-40, *Internal-Use Software*, may be applicable to cybersecurity expenditures. Following a cyber-incident, the Staff noted, ASC 605-50, *Customer Payments and Incentives*, might apply to efforts to maintain business relationships, or ASC 450-20, *Loss Contingencies*, may determine whether potential liabilities to third parties should be recognized. In addition, a company might need to consider whether long-lived assets such as goodwill or capitalized software have been impaired and subsequently reassess underlying assumptions.



LOEB & LOEB adds Depth.

Disclosure Controls and Procedures

If a cyber-incident could affect a company's ability to record, process, summarize, and report information required to be included in a report filed with the SEC, the company should consider whether the risk of a cyber-incident impairs the effectiveness of the Company's disclosure controls and procedures.

This client alert is a publication of Loeb & Loeb LLP and is intended to provide information on recent legal developments. This client alert does not create or continue an attorney client relationship nor should it be construed as legal advice or an opinion on specific situations. For more information on the content of this alert, please contact [David C. Fischer](#) or any other member of Loeb & Loeb's Corporate Group.

Circular 230 Disclosure: To assure compliance with Treasury Department rules governing tax practice, we inform you that any advice (including in any attachment) (1) was not written and is not intended to be used, and cannot be used, for the purpose of avoiding any federal tax penalty that may be imposed on the taxpayer, and (2) may not be used in connection with promoting, marketing or recommending to another person any transaction or matter addressed herein.

This publication may constitute "Attorney Advertising" under the New York Rules of Professional Conduct and under the law of other jurisdictions.

© 2011 Loeb & Loeb LLP. All rights reserved.