Advisory
SECURITIES & CAPITAL MARKETS PRACTICE GROUP | FEBRUARY 2012

WIGGIN AND DANA
Counsellors at Law

SEC's Division of Corporation Finance Issues Guidance on Cybersecurity Disclosure

Companies are becoming increasingly dependent on digital technologies in the operation of their businesses. At the same time, data security breaches and other "cyber incidents" have become more frequent and severe. Consequently, it has become imperative that public companies understand how cybersecurity risks and cyber incidents should be described within the framework of the disclosure obligations imposed by federal securities laws.

In the wake of recent high-profile data security breaches, several senators led by Senator John D. Rockefeller IV (D-WV) sent a letter to Mary Schapiro, Chairman of the Securities and Exchange Commission (the "SEC"), requesting that the SEC "publish interpretive guidance clarifying existing disclosure requirements pertaining to information security risk."[1] In response to this letter, the SEC's Division of Corporation Finance issued "CF Disclosure Guidance: Topic No. 2" (the "Disclosure Guidelines").[2] The Disclosure Guidelines provide interpretive guidance to all registrants regarding the disclosure obligations related to cybersecurity risks and cyber incidents.

The Disclosure Guidelines define cybersecurity as "the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access." The Disclosure Guidelines note that the objectives of a cyber attack may include corrupting data, causing operation disruption or misappropriating financial assets, intellectual property or other sensitive information. If such a cyber incident occurs, the consequences could be severe and the damages could include remediation costs, increased cybersecurity protection costs, lost revenues, litigation expenses and reputational damage.

While there are no existing disclosure rules that specifically address cybersecurity risks and cyber incidents, the Disclosure Guidelines provide an overview of the sections of public filings where existing disclosure obligations may require registrants to discuss cybersecurity risks and cyber incidents.

- **Risk Factors.** In accordance with Item 503(c) of Regulation S-K, a registrant is required to "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 registrant should take into account prior cyber incidents, the severity and frequency of those incidents and the adequacy of preventative measures in determining whether risk factor disclosure is required. A registrant should evaluate the likelihood that a cyber incident could occur and the magnitude of the impact a cyber incident could have on its business. Appropriate disclosures may include descriptions of the:
  - aspects of the business that give rise to material cybersecurity risks and the potential consequences;
  - material cybersecurity risks associated with outsourcing functions and how the registrant addresses those risks;
  - material cyber incidents experienced and the consequences of those incidents;
  - risks relating to undetected cyber incidents; and
  - insurance coverage.

continued next page

If you have any questions about this Advisory, please contact:

Michal Grundei
203.363.7630
mgrundei@wiggin.com

Mark S. Kaduboski
203.363.7627
mkaduboski@wiggin.com

Scott Kaufman
212.551.2639
skaufman@wiggin.com

Kristin B. Flood
203.363.7619
kflood@wiggin.com

About the Securities and Capital Markets Practice Group

Broadly experienced in public offerings and private placements of securities, Exchange Act compliance, PIPE transactions, angel and venture capital financings, bond finance, and other areas of equity and debt financing, our veteran Securities and Capital Markets Group provides sophisticated, innovative and market-savvy counsel to NYSE, NASDAQ and NYSE Amex-listed companies, emerging companies, underwriters, venture capital firms, and hedge funds.

In certain jurisdictions this may constitute attorney advertising. © 2012 Wiggin and Dana LLP

WIGGIN AND DANA

Counsellors at Law

This publication is a summary of legal principles. Nothing in this article constitutes legal advice, which can only be obtained as a result of a personal consultation with an attorney. The information published here is believed accurate at the time of publication, but is subject to change and does not purport to be a complete statement of all relevant issues.

- **Management's Discussion and Analysis of Financial Condition and Results of Operations** ("**MD&A**"). In accordance with Item 303 of Regulation S-K, a registrant is required to disclose cybersecurity risks and cyber incidents in its MD&A if the costs or other consequences associated with such risks or 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 reported financial information not to be necessarily indicative of future operating results or financial condition."

- **Description of Business.** Pursuant to Item 101 of Regulation S-K, a registrant should discuss cybersecurity risks and cyber incidents in its "Description of Business" if such risks or incidents materially affect its products, services, relationships or competitive conditions.

- **Legal Proceedings**. If a cyber incident results in a material legal proceeding involving a registrant, the registrant would need to describe the proceeding in its "Legal Proceedings" disclosure in accordance with Item 103 of Regulation S-K.

- **Financial Statement Disclosure.** Cybersecurity risks and cyber incidents may affect financial statements in a variety of ways including by creating a need to recognize:

  - capitalization of costs associated with cybersecurity;

  - use of incentives to mitigate damages from a cyber incident;

  - losses stemming from asserted and unasserted claims related to cyber incidents; and

  - impairment of assets including goodwill, customer-related intangible assets, trademarks, patents, inventory, capitalized software or other long-lived assets associated with hardware or software.

  If a cyber incident is discovered after the balance sheet date but before the issuance of financial statements, the registrant should evaluate whether disclosure of a recognized or non-recognized subsequent event is required.

- **Other Considerations.** Material information regarding cybersecurity risks and cyber incidents must also be disclosed "when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading."

The Disclosure Guidelines do not create additional disclosure obligations or expand existing disclosure obligations. The purpose of the Disclosure Guidelines is merely to provide interpretative guidance on the application of the federal securities laws to a "hot topic" in the headlines.

The Disclosure Guidelines do, however, signal an increased emphasis by the SEC on cybersecurity and accordingly, registrants should review their disclosures to ensure that they include appropriate discussions of cybersecurity risks and cyber incidents consistent with the Disclosure Guidelines. The complete text of the Disclosure Guidelines can be found here.

---

[1] Letter from Senator John D. Rockefeller IV to Mary Schapiro, Chairman of the United States Securities and Exchange Commission (May 11, 2011), available at http://commerce.senate.gov/public/?a=Files.Serve&File_id=4ceb6c11-b613-4e21-92c7-a8e1dd5a707e.

[2] Division of Corporation Finance, Securities and Exchange Commission, CF Disclosure Guidance, Topic No. 2: Cybersecurity (Oct. 13, 2011), available at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.