2013 Conference on Securities Regulation and Business Law

February 7-8, 2013
Austin, TX

SEC DISCLOSURE GUIDANCE ON CYBERSECURITY RISKS

Christopher J. Volkmer
Volkmer-Reid Law Firm PLLC

SEC DISCLOSURE GUIDANCE ON CYBERSECURITY RISKS

Christopher J. Volkmer
Volkmer-Reid Law Firm PLLC

I. Setting the Stage

On October 13, 2011, the Securities and Exchange Commission ("SEC") issued guidance on disclosure issues associated with "Cybersecurity" risks of registrants. It is the first such guidance by the SEC, and it highlights the dependency of many businesses on data to derive investor value. Indeed, one only has to look at the astronomical growth of Google, Inc. and Facebook to as new public entities to appreciate the importance of data security to the investing public. The issuance of this guidance appears to be at the prompting of a letter from five Senators, including Jay Rockefeller, the Chair of the Committee on Commerce, Science, and Transportation to Mary Shapiro, the SEC Chairman. The letter is dated May 11, 2011, and requests that the SEC provide issuers with guidance in the area of Cybersecurity, and offers the concern that "the lack of quality, public information in these matters enables an inefficient marketplace that devalues security and impairs investor decision-making."[1] Clearly, the focus of the Committee is not so much the issue of personally identifiable information as the effect of security breaches on the corporate marketplace, and in turn, the investors who invest in commercial entities. Chairman Shapiro responded in a letter dated June 6, 2011, reviewing the existing reporting obligations of public companies, but also promising to review whether additional guidance is necessary. The SEC issued its guidance five months later.

For lawyers, the SEC guidance throws light on the nature and extent of regulatory oversight in this area, the current litigation environment, the adoption of new technologies that create risk for public reporting clients, and how such risks should be disclosed. The goal of this paper is to summarize the SEC guidance on Cybersecurity and to provide some insights into how the guidance should be considered in light of certain legal, policy, and technological requirements.

II. The SEC Disclosure Guidance

A. Introduction

The CF Disclosure Guidance: Topic No. 2 was issued by the Division of Corporation Finance of the SEC on October 13, 2011.[2] The statements in the Guidance do not constitute a rule or regulation and it is neither approved nor disapproved by the SEC.[3] The Guidance is intended to be consistent with relevant disclosure concerning other business risks, but the SEC specifically notes in the introduction[4] that it is not requiring registrants to include information that will give third parties a "roadmap" to how a breach the registrant's security systems.

[1] The letter of the Senators and the reply letter from Chairman Shapiro are attached to this paper.
[2] Available at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (the "Guidance").
[3] Guidance, Supplementary Information.
[4] Guidance, Introduction, ¶2.

The topic of the guidance is "Cybersecurity" which the Guidance defines as follows:

> Cybersecurity is the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access.[5]

By using this definition, the SEC seems to be focused on not just the data of a registrant (as the term "data security" might suggest) but also the "digital technologies [used] to conduct their operations." [6] Thus, while the popular notion of security focuses on the risks associated with the compromise of data (and particularly of personally identifiable data), the Guidance includes the risks to digital technology systems on which the business has a dependency. In this regard, the Guidance notes that the objects of the threats to network security of a registrant may vary widely, including theft of financial assets, intellectual property, sensitive company or customer information, or disruption of business operations. [7] Note also, however, that the Guidance uses the undefined term "cyber incident" over 25 times. While one may presume that this should be taken in an ordinary sense of an event relating to Cybersecurity, but as discussed in greater detail below, the question of what exactly is a "cyber incident" raises some interesting questions. Moreover, the scope of risk for will be important when considering the specific guidance on disclosure obligations, also as discussed below.

In its introductory remarks, the Guidance also notes "substantial costs and other negative consequences" and lists the following as examples:

- Remediation costs that may include liability for stolen assets or information and repairing system damage that may have been caused. Remediation costs may also include incentives offered to customers or other business partners in an effort to maintain the business relationships after an attack;
- Increased Cybersecurity protection costs that may include organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;
- Lost revenues resulting from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- Litigation; and
- Reputational damage adversely affecting customer or investor confidence. [8]

While these categories of costs are very inclusive, it will be discussed later in this article whether a Cybersecurity incident would rise to the level of materiality for a public company.

---

[5] Guidance, Introduction ¶1 at endnote 1 (citing http://whatis.techtarget.com/definition/Cybersecurity.html and http://www.merriam-webster.com/dictionary/Cybersecurity).
[6] Guidance, Introduction, ¶1.
[7] Guidance, Introduction, ¶4.
[8] Ibid.

Title search: SEC Disclosure Guidance on Cybersecurity Risks

First appeared as part of the conference materials for the
35th Annual Securities Regulation and Business Law session
"Cyber Security for the Securities Lawyer"