SEC Provides Guidance on Cybersecurity Risks and Cyber Incidents

On October 13, 2011, the Division of Corporation Finance of the Securities and Exchange Commission (the "SEC") issued Disclosure Guidance providing the Division's views on disclosure obligations relating to cybersecurity risks and cyber incidents.[1] Although the Guidance focuses on one type of risk, the analysis of disclosure obligations also applies to business and operational risks generally. The Guidance notes that SEC registrants have become increasingly dependent on digital technologies, which has increased the significance of cybersecurity risks and cyber incidents, such as denial-of-service attacks on websites or unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. The Division highlights costs and negative consequences from cyber incidents that could require discussion under existing disclosure obligations, including:

- remediation costs, including liability for stolen assets or information, repairing system damage or incentives to customers or business partners to maintain business relationships;
- increased cybersecurity protection costs;
- lost revenues due to misuse of proprietary information or loss of customers;
- litigation; and
- reputational damage adversely affecting customer or investor confidence.

I. Disclosure Requirements Applicable to Cybersecurity Risks

Although the Division notes that no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents in registration statements for securities offerings and in annual and quarterly reports. The Guidance is consistent with previous SEC interpretations of disclosure requirements that arise generally in connection with business, operational and financial risks.[2] The Division also emphasizes that, although existing disclosure obligations may require discussion of cybersecurity risks and incidents, registrants are not required to provide disclosures that could compromise cybersecurity efforts — for example, by providing a "roadmap" for those who seek to infiltrate a registrant's network security.

General Requirements to Disclose Material Information

In addition to the information expressly required by SEC regulations, Forms or Schedules, registrants are also required to disclose such further material information, if any, as may be necessary to make the required

---

1 See SEC Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2, Cybersecurity (October 13, 2011), available at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

2 See, e.g., Commission Guidance Regarding Disclosure Related to Climate Change, SEC Release No. 33–9106, 75 Fed. Reg. 6290 (Feb. 2, 2010), available at http://www.sec.gov/rules/interp/2010/33-9106fr.pdf; and SEC interpretive guidance on disclosure requirements for management's discussion and analysis, including: Commission Guidance Regarding Management's Discussion and Analysis of Financial Condition and Results of Operations, SEC Release No. 33-8350, 68 Fed. Reg. 75056 (Dec. 19, 2003), available at http://www.sec.gov/rules/interp/33-8350.htm, and prior SEC Releases on management's discussion and analysis referred to therein. See also Firm Memorandum, Cahill Gordon & Reindel LLP, SEC Publishes Interpretive Release on Disclosure Relating to Climate Change (Feb. 5, 2010).

statements, in light of the circumstances under which they are made, not misleading.[3] Information is considered material if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision or if the information would significantly alter the total mix of information made available.[4]

Risk Factors

Existing disclosure rules require registrants to disclose risk factors in registration statements for securities offerings and in annual and quarterly reports on Forms 10-K and 10-Q. Item 503 of Regulation S-K requires risk factor disclosure for the most significant factors that make an investment in the registrant speculative or risky. To determine whether risk factor disclosure is required, registrants should evaluate their cybersecurity risks, including the severity and frequency of prior cybersecurity incidents and threats, as well as the probability and magnitude of cybersecurity incidents and preventative measures taken. The Guidance identifies examples of risk factor disclosure that registrants should consider, including discussion of:

- aspects of a registrant's business that are subject to cybersecurity risks and potential costs and consequences;
- outsourced functions with cybersecurity risks and actions to address those risks;
- material cybersecurity incidents experienced by the registrant and their costs and consequences;
- risks due to potential undetected cybersecurity incidents; and
- relevant insurance coverage.

Risk factor disclosure must adequately describe the nature of the material risks and specify how each risk affects the registrant. Generic or boilerplate risk factor disclosure that could apply to any issuer or any offering should be avoided in the view of the SEC. However, the Division emphasizes that disclosures are not required to be so detailed that they provide a roadmap to compromise registrants' cybersecurity.

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

As with other business risks, a registrant should include discussion of cybersecurity risks and cyber incidents in the MD&A sections of its filings, pursuant to Item 303 of Regulation S-K, if the costs or 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 reported financial information not to be necessarily indicative of future operating results or financial condition.

---

[3] See Securities Act Rule 408, Exchange Act Rule 12b-20 and Exchange Act Rule 14a-9.

[4] See *Basic Inc. v. Levinson*, 485 U.S. 224 (1988); and *TSC Industries, Inc. v. Northway, Inc.*, 426 U.S. 438 (1976).

The Guidance provides examples of situations that could require MD&A discussion: for example, if material intellectual property is stolen in a cyber attack and the effects of the theft are reasonably likely to be material, then the registrant should describe the property that was stolen and the effect of the attack on its results of operations, liquidity, and financial condition, as well as reasonably likely increases in cybersecurity protection or litigation costs, including the amount and duration of expected costs, if material. Similarly, a registrant should discuss material increases in cybersecurity protection expenditures in response to a cybersecurity incident, even if no loss of intellectual property occurred.

Description of Business

The Division explains that a registrant should also provide disclosure in the "Description of Business" sections of its filings, pursuant to Item 101 of Regulation S-K, if cybersecurity incidents materially affect its products, services, relationships with customers or suppliers, or competitive conditions, considering the impact on each of the registrant's reportable segments. For example, if a registrant learns of a cybersecurity incident that could materially impair the viability of a new product in development, then it should discuss the incident and the potential impact to the extent material.

Legal Proceedings

As with other risks, the Guidance notes that if a cybersecurity incident leads to material litigation, other than certain ordinary routine litigation incidental to a registrant's business, the registrant would need to disclose information regarding the litigation in its "Legal Proceedings" disclosure, pursuant to Item 103 of Regulation S-K. The registrant would need to briefly describe the litigation, including the name of the court or agency in which the proceedings are pending, the date instituted, the principal parties thereto, a description of the factual basis alleged to underlie the proceeding and the relief sought.

Financial Statement Disclosures

The Guidance notes that cybersecurity risks and incidents could significantly impact a registrant's financial statements, and identifies accounting standards that registrants may need to consider, depending on the nature and magnitude of risks or incidents. The Division provides examples, including: costs for preventative measures related to internal-use software are addressed by Accounting Standards Codification ("ASC") 350-40, *Internal-Use Software*, and registrants should consider ASC 605-50, *Customer Payments and Incentives*, in connection with customer incentives to maintain business relationships following a cybersecurity incident.

Consistent with recent emphasis by the Division,[5] the Guidance notes that loss contingency disclosure may be required in connection with cybersecurity incidents that could result in 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. The Division indicates that registrants should refer to ASC 450-20, *Loss Contingencies*, (formerly SFAS 5) to determine when to recognize a liability if those losses are probable and reasonably estimable. In addition, the Guidance states that registrants must provide certain disclosures with respect to losses that are at least reasonably possible.

---

[5] See, e.g., Wayne Carnall, Chief Accountant, Division of Corporation Finance, Remarks before the 2010 AICPA National Conference on Current SEC and PCAOB Developments, Washington, D.C., (Dec. 7, 2010) (Slide Presentation), available at http://www.sec.gov/news/speech/2010/spch120710wc.pdf; and Sample Letter Sent to Public Companies on Accounting and Disclosure Issues Related to Potential Risks and Costs Associated with Mortgage and Foreclosure-Related Activities or Exposures (October 2010), available at http://www.sec.gov/divisions/corpfin/guidance/cfoforeclosure1010.htm.

If cybersecurity incidents result in diminished future cash flows, registrants may need to consider the possibility of charges for impairment of assets, including goodwill, customer-related intangible assets, trademarks, patents, capitalized software or other long-lived assets associated with hardware or software, and inventory. Registrants may be required to develop, and subsequently reassess, estimates to account for the financial implications and to explain risks or uncertainties of reasonably possible changes in their estimates that would be material to their financial statements. The Guidance indicates that examples of such estimates include estimates of warranty liability, allowances for product returns, capitalized software costs, inventory, litigation and deferred revenue.

The Guidance also indicates that a cybersecurity incident discovered after the balance sheet date but before the issuance of financial statements may require disclosure of a recognized or nonrecognized subsequent event. 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

Registrants are required to disclose conclusions on the effectiveness of disclosure controls and procedures. If cybersecurity incidents pose a risk to a registrant's ability to record, process, summarize, and report information required to be disclosed in SEC filings, management should also consider whether there are deficiencies in disclosure controls and procedures that would render them ineffective.

II. Conclusion

The Disclosure Guidance provides the Division's views on disclosure obligations relating to cybersecurity risks and cyber incidents and continues the Division's emphasis on loss contingency disclosures and disclosure requirements that are generally applicable to business and operational risks. Registrants should consider the disclosure obligations and analysis outlined in the Guidance when preparing annual and quarterly reports or registration statements for securities offerings.

* * *

If you have any questions about the issues addressed in this memorandum or if you would like a copy of any of the materials mentioned, please do not hesitate to call or email Charles A. Gilman at 212.701.3403 or cgilman@cahill.com; Jon Mark at 212.701.3100 or jmark@cahill.com; John Schuster at 212.701.3323 or jschuster@cahill.com; or Dan Zimmerman at 212.701.3777 or dzimmerman@cahill.com.