DORSEY™
DORSEY & WHITNEY LLP
USA CANADA EUROPE ASIA-PACIFIC

A NEW CENTURY OF SERVICE 1912 | 2012

Christopher L. Doerksen
Partner
(206) 903-8856
Email

October 20, 2011

SEC Issues Interpretive Guidance on Cybersecurity Disclosures

In response to the increasing frequency and severity of cybersecurity incidents, the staff of the Securities and Exchange Commission ("SEC") has issued interpretive guidance for registrants to assist them in assessing what, if any, disclosures should be provided in periodic reports and registration statements about cybersecurity matters in light of each registrant's specific facts and circumstances.

Background

As registrants have migrated toward increasing dependence on digital technologies to conduct their operations, the risks to registrants associated with the security of such technologies, known as cybersecurity, have also increased. Registrants have been subject to both intentional and inadvertent cyber incidents, such as unauthorized release of proprietary or sensitive information, misappropriation of assets, corruption of data and loss of service, resulting in costs and liability, lost revenues, litigation and reputational damage.

Required Disclosures

The staff's new guidance does not change existing disclosure standards, but provides a useful reminder to registrants that cybersecurity matters may require disclosures of the following nature:

- Risk factors – if the risk of cybersecurity incidents or the consequences of preventative or remedial actions are among the most significant factors that make an investment in the company speculative or risky.
- Results of operations (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 the company'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 – if cyber incidents have had a material effect on the company's (or any reportable segment's) products, services, relationships with customers or suppliers, or competitive conditions.
- Legal proceedings – if a material pending legal proceeding involves a cyber incident.
- Disclosure controls and procedures – if cyber incidents pose a risk to a company's ability to record, process, summarize and report information that is required to be disclosed in SEC reports that is sufficient to render the company's controls

ineffective.
- Form 8-K or 6-K reports – if a cyber incident results in a reportable event, or if additional disclosures are required in order to maintain the accuracy and completeness of information in effective shelf registration statements.

The staff also provides guidance regarding the effect that cybersecurity matters may have on financial statements.

Action Items

Registrants should:

- Assess whether the company's current disclosures regarding cybersecurity issues are adequate, in light of the company's exposure to cybersecurity risks, the existence and effect of any known cyber incidents, the status of its cybersecurity measures, its industry and the disclosures made by similarly-situated companies;
- Be prepared for the disclosures that may be necessary following a cyber incident; and
- Consider cybersecurity issues in connection with management's periodic evaluation of the effectiveness of the company's disclosures controls and procedures.

A complete copy of the staff's guidance can be found here.