LEGAL UPDATES

PUBLISHED: OCTOBER 24, 2011

Cybersecurity Threats and Vulnerabilities May Require Disclosure

Service

Securities & Corporate Governance

Professional

KIRSTIN P. SALZMAN
KANSAS CITY:
816.983.8316
KIRSTIN.SALZMAN@
HUSCHBLACKWELL.COM

Recent guidance from the SEC's Division of Corporate Finance (Division) advises public companies to assess, on an ongoing basis, the need to disclose cybersecurity risks and cyber incidents within the context of existing disclosure requirements connected with any business risk that could materially impact the company's operations. The guidance does not create a new disclosure requirement specific to cybersecurity nor does it contemplate disclosures that could compromise a registrant's efforts to prevent cyber attacks. Instead, the Division identifies several sections of the periodic reports that may require discussion of cybersecurity issues based on existing disclosure standards.

Risk Factors

The guidance instructs companies 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" and identifies the following factors to be used in evaluating the need for disclosure based upon all relevant information, including past incidents:

The likelihood that a cyber incident will occur;

The qualitative and quantitative magnitude of the risks, including the potential costs and other consequences associated with the misappropriation of assets or sensitive information, data corruption or disruption in operations; and

The sufficiency of preventative actions taken to reduce risks within the context of the industry in which the company operates and risks to its security, including threatened attacks of which the company is aware.

If these considerations lead to the conclusion that disclosure is warranted, the disclosure should adequately describe the nature of the material risk and how the risk affects the registrant. The guidance suggests that the following factors should be addressed:

Any aspects of the company's business or operations that give rise to material cybersecurity risks and the potential costs and consequences;

A description of any outsourced functions that have material cybersecurity risks;

A description of any actual cyber incidents that were individually or collectively material, including a description of the costs and other consequences;

Risks related to cyber incidents that may be undetected for an extended period; and

A description of any relevant insurance coverage.

MD&A

According to the guidance, the company should also discuss cybersecurity risks and incidents in the MD&A if "the costs or other 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."

Business Description and Legal Proceedings

The guidance directs that if one or more cyber incidents materially affect a company's products, services, relationship with customers or suppliers, or competitive conditions, the company should disclose the incident and its impacts in the "Description of Business" section. Additionally, if the company is a party to a material pending legal proceeding that involves a cyber incident, the company may need to reveal information about the incident in its "Legal Proceedings" disclosure.

Financial Statement Disclosures

The guidance describes several ways in which cybersecurity risks or cyber incidents could impact the company's financial statements before, during and after an attack or event.

Disclosure Controls and Procedures

If cyber incidents expose any deficiencies in a company's disclosure controls and procedures that render them ineffective, the deficiencies will need to be disclosed.

What This Means to You

Any company utilizing digital technologies to conduct their operations is vulnerable to cyber attacks that could result in material impacts that range from present to future financial losses as well as impairments to assets such as goodwill, customer-related intangible assets, intellectual property, hardware, software, inventory, etc. Depending on the nature and severity of these potential or actual risks, they could have a broad impact on a public company's financial statements. Therefore, management is advised to review cybersecurity measures on an ongoing basis and be prepared to address any vulnerability that could have a material impact upon the company's operations. Additionally, management should plan to assess the effect of any cyber incident and develop estimates to account for various financial implications.

Contact Info

If you have any questions about this new guidance or any other issue related to securities law, please contact your Husch Blackwell attorney.

Husch Blackwell LLP regularly publishes updates on industry trends and new developments in the law for our clients and friends. Please contact us if you would like to receive updates and newsletters, or request a printed copy.