MAYER·BROWN

Legal Update
November 11, 2011

SEC Issues Guidance on Disclosure Obligations Relating to Cybersecurity Risks and Cyber Incidents

In light of the increased dependence on digital technologies by public companies and the increasing frequency and severity of cyber incidents, the Division of Corporation Finance of the Securities and Exchange Commission (the "SEC") issued guidance on October 13, 2011, regarding the disclosure obligations of public companies relating to cybersecurity risks and cyber incidents. In preparing its guidance, the SEC Staff tried to balance the disclosure obligations of public companies against the potential for detailed disclosures to compromise cybersecurity efforts by providing a roadmap for those seeking to infiltrate a public company's network security.

CF Disclosure Guidance: Topic No. 2

Rather than creating new disclosure requirements, the guidance describes how existing requirements should be interpreted and includes some examples for consideration. Although not intended to be exhaustive, the SEC guidance focused on the following six disclosure areas.

RISK FACTORS

Issues for public companies to consider when determining whether risk factor disclosure should be made, include the frequency and severity of prior cybersecurity incidents, the likelihood of future such incidents and the quantitative and qualitative magnitude of any incidents, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption. Public companies should also consider the adequacy of their preventative actions taken – particularly in the context of the industries in which they operate.

The SEC Staff noted that, in particular circumstances, disclosures may need to include a description of

- Aspects of the business that give rise to material cybersecurity risks and the potential costs and consequences;
- Cyber incidents experienced by the public company, including a description of the costs and other consequences;
- The risks related to cyber incidents that may remain undetected for an extended period; and
- Relevant insurance coverage.

MANAGEMENT'S DISCUSSION AND ANALYSIS OF FINANCIAL CONDITION AND RESULTS OF OPERATIONS

The SEC Staff stated that public companies "should address cybersecurity risks and cyber incidents in this MD&A if the costs or other consequences associated with one or more known incidents or other risk of potential incidents represent a material event, trend or uncertainty that is reasonably likely to have a material effect on the [public company's] results of operation, 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

A public company should provide disclosure in its "Business" discussion if one or more cyber incidents materially affected its products, services, customer or supplier relationships or competitive conditions – either with respect to the company as a whole or one of its material reportable segments.

LEGAL PROCEEDINGS

If a public company has been sued as a result of a cyber incident, it may need to disclose the litigation in its "Legal Proceedings" discussion. This disclosure would include the name of the court in which the proceedings are pending, the date the litigation was instituted, the principal parties and a description of the factual basis alleged to underlie the proceeding and the relief sought.

FINANCIAL STATEMENTS

The SEC Staff highlighted several accounting requirements that may be applicable.

If a public company incurs substantial costs related to internal use software to prevent cyber incidents, the capitalization of these costs is addressed by Accounting Standards Codifications ("ASC") Topic 350-40, *Internal-Use Software*.

If a public company provides incentives to customers to mitigate damages from a cyber incident, the recognition, measurement and classification of these incentives is addressed by ASC Topic 605-50, *Customer Payments and Incentives*.

If a public company might experience losses resulting from asserted and unasserted claims due to a cyber incident – including claims relating to warranties, breach of contract, product recall and replacement and indemnification – the recognition of liabilities and other required disclosures is addressed by ASC Topic 450-20, *Loss Contingencies*.

In the event of a cyber incident, a public company must consider whether certain assets – including goodwill, customer-related intangible assets, trademarks, patents, capitalized software, inventory or other long-lived assets associated with hardware or software, have been impaired. If they have been impaired, the disclosures surrounding any risk or uncertainty of a reasonably probable near-term change in the estimates used in the impairment analysis is addressed by ASC Topic 275-10, *Risks and Uncertainties*.

If a cyber incident is discovered after a balance sheet date but before the financial statements for that period have been issued, whether disclosure of the event as a subsequent event is required is addressed by ASC Topic 855-10, *Subsequent Events*.

DISCLOSURE CONTROLS AND PROCEDURES

If a cyber incident poses a risk to a public company's ability to record, process, summarize and report information that is required to be disclosed in filings made with the SEC, management must consider whether there are any deficiencies in the company's disclosure controls and procedures that would render those disclosure controls and procedures ineffective, and, if they are ineffective, provide the additional disclosures the SEC rules by such a conclusion.

Implications of the Disclosure Guidance

As a result of the SEC Staff's disclosure guidance, public companies should reassess the adequacy of their disclosures concerning cybersecurity risks and cyber incidents. This should not be a one time review, but should be made a part of the regular disclosure process so that evolving circumstances are appropriately and timely reflected in the disclosures made in filings with the SEC. ◆

If you have any questions regarding the SEC Guidance on Disclosure Obligations Relating to Cybersecurity Risks and Cyber Incidents, *please contact the author of this Legal Update, Michael L. Hermsen, at +1 312 701 7960, or any of the lawyers listed below or any other member of our Corporate & Securities group.*

David S. Bakst
+1 212 506 2551
dbakst@mayerbrown.com

John P. Berkery
+1 212 506 2552
jberkery@mayerbrown.com

Paul C. de Bernier
+44 20 3130 3232
pdebernier@mayerbrown.com

Edward S. Best
+1 312 701 7100
ebest@mayerbrown.com

Robert E. Curley
+1 312 701 7306
rcurley@mayerbrown.com

Marc H. Folladori
+1 713 238 2696
mfolladori@mayerbrown.com

Robert F. Gray, Jr.
+1 713 238 2600
rgray@mayerbrown.com

Lawrence R. Hamilton
+1 312 701 7055
lhamilton@mayerbrown.com

Michael L. Hermsen
+1 312 701 7960
mhermsen@mayerbrown.com

Philip J. Niehoff
+1 312 701 7843
pniehoff@mayerbrown.com

Elizabeth A. Raymond
+1 312 701 7322
eraymond@mayerbrown.com

Laura D. Richman
+1 312 701 7304
lrichman@mayerbrown.com

David A. Schuette
+1 312 701 7363
dschuette@mayerbrown.com

Jodi A. Simala
+1 312 701 7920
jsimala@mayerbrown.com

Frederick B. Thomas
+1 312 701 7035
fthomas@mayerbrown.com