October 20, 2011

Cybersecurity: SEC Staff Provides Guidance on Disclosure Considerations

The staff of the SEC's Division of Corporation Finance recently issued Disclosure Guidance on cybersecurity risks. The guidance does not impose any new disclosure obligations but rather frames cybersecurity as a business risk that, like other operational and financial risks, may call for disclosure if it could materially impact a company's operations.

The staff's issuance of the guidance follows a request made by several Senators, led by Senator John D. Rockefeller IV, last spring that the staff publish guidance clarifying existing disclosure requirements pertaining to informational security risk. (The Senators' letter to SEC Chairman Mary Schapiro is here. Chairman Schapiro's response letter is here).

The Senators' focus on this issue and several publicized cyber incidents have clearly brought cybersecurity to the forefront. Given the public nature of this matter and the staff's issuance of the guidance in the midst of its heavy regulatory agenda, we would not be surprised to see the staff issue more comments in this area going forward. Whether and what companies disclose about cybersecurity risk, however, will remain a facts and circumstances analysis highly dependent upon a company's business characteristics and risk profile.

What is Cybersecurity?

The guidance describes cybersecurity as the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access. Cyber incidents can result from deliberate or unintentional events and may involve unauthorized or authorized access to digital systems in order to misappropriate sensitive information, corrupt data or cause operational disruption. The guidance indicates that companies, depending upon their business model, may be subject to material cybersecurity risks associated with:

- remediation costs related to stolen assets or information, repairing system damage and incentives offered to maintain business relationships after an attack;
- increased cybersecurity protection costs;
- lost revenues resulting from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- litigation; and
- reputational damage.

Risk Factors

The guidance directs companies to provide risk factor disclosure related to cyber incidents *if these issues are among the most significant factors that make an investment in the company speculative or risky* (emphasis added). In determining whether and what to disclose about cybersecurity risks, the guidance advises companies to consider:

- the probability that cyber incidents will occur;
- the quantitative and qualitative magnitude of cybersecurity risks, including the costs and consequences arising from the misappropriation or corruption of data or operational disruption; and

- the adequacy of preventative actions taken to reduce known and unknown cybersecurity risks.

If risk factor disclosure is called for, the company should consider addressing:

- aspects of the company's business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- to the extent the company outsources functions that have material cybersecurity risks, a description of those functions and how the company addresses those risks;
- specific cyber incidents that have been material individually or in the aggregate and the related consequences and costs;
- risks related to cyber incidents that remain undetected for an extended period; and
- relevant insurance coverage.

MD&A

The guidance suggests that MD&A disclosure of cybersecurity matters may be necessary if the costs or other consequences associated with one or more cyber incidents represent a material event, trend or uncertainty that is reasonably likely to have a material effect on the company's operations, liquidity or financial condition or would cause reported financial information not to be necessarily indicative of future results. For example, if material intellectual property is stolen in a cyberattack, a company might describe the stolen property, the effect of the attack on its results of operations, liquidity, and financial condition and the potential impact of the attack on the company's future results. Alternatively, if the attack did not result in the loss of intellectual property but prompted the company to materially increase its cybersecurity protection expenditures, the guidance urges the company to discuss those increased expenditures.

Business and Legal Proceedings

The guidance says that disclosure may be called for in the Business section of a company's SEC filings if one or more cyber incidents materially affect a company's products, services, relationships with customers or suppliers, or competitive conditions. These disclosure considerations should involve an assessment of the impact of the cybersecurity event on each of the company's reportable segments. If a significant amount of customer information is stolen, resulting in material litigation, the company should disclose the material litigation in the Legal Proceedings section of its filings.

Financial Statements and Disclosure Controls & Procedures

The guidance also points out some ways cybersecurity incidents or the risk thereof may impact a company's financial statements both before, during and after a cyber event. For example, companies may incur costs to prevent cyber events or mitigate damages due to an event and may experience diminished cash flows as a result of an event. The guidance also directs companies to consider whether any asserted and unasserted claims related to the cyber incident ought to be disclosed or accrued for. Companies should also take cyber incidents, or the threat thereof, into account when evaluating the effectiveness of their disclosure controls & procedures.

Conclusion

The cybersecurity guidance provides a helpful outline for companies, including those outside of industries that have traditionally focused on cybersecurity issues, to use when assessing whether they have adequately disclosed their vulnerability to cyber incidents. As the guidance implies, cybersecurity disclosure will not be appropriate for all companies and companies should avoid "boilerplate" disclosure in this area. The guidance is also explicit that the federal securities laws do not require disclosure which itself would compromise a company's cybersecurity or provide a "roadmap" for those who seek to infiltrate

a company's network security. Given the public and staff interest in the topic, however, we suggest that companies utilize the guidance as an opportunity to reconsider their disclosure in this area.

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

Julia K. Cowles	650 752 2007	julia.cowles@davispolk.com
Joseph A. Hall	212 450 4565	joseph.hall@davispolk.com
Michael Kaplan	212 450 4111	michael.kaplan@davispolk.com
Richard J. Sandler	212 450 4224	richard.sandler@davispolk.com
Richard D. Truesdell, Jr.	212 450 4674	richard.truesdell@davispolk.com
Janice Brunner	212 450 4211	janice.brunner@davispolk.com