Client Update

SEC Issues New Guidance on Public Company Cybersecurity Disclosure and Governance

Yesterday, the SEC issued new Guidance regarding cybersecurity disclosure requirements under the federal securities laws applicable to SEC reporting companies. The Guidance reinforces and expands upon October 2011 guidance issued by the staff of the Division of Corporation Finance.[1]

The Guidance addresses two topics not covered in the 2011 guidance: (1) the importance of developing comprehensive controls and procedures related to cybersecurity, including those intended to facilitate an assessment of the materiality of—and consequent disclosure obligations stemming from—cybersecurity risks and incidents; and (2) the need for policies and procedures to guard against trading by insiders based on material non-public information about cyber incidents or risks and to ensure the timely disclosure of related material information.

SEC reporting companies with calendar-year fiscal years that are currently preparing 10-K and proxy disclosure should, assuming time allows, review the Guidance before finalizing their filings.

CYBERSECURITY GUIDANCE

Building on the 2011 guidance, the Guidance underscores the importance of robust and timely disclosure of cybersecurity incidents and risks, emphasizing that boilerplate disclosures (e.g., we "may" be the victim of a distributed denial of service ("DDoS") attack) are likely insufficient where the company has in fact experienced an incident (e.g., it has been the victim of a DDoS attack). The Guidance recognizes that disclosures need not reveal sensitive information about the company's protective measures—lest they provide a roadmap to attackers—and suggests that companies consider the following factors when assessing disclosure obligations:

[1] The Guidance is available here.

- The nature, extent, and potential magnitude of the risks and incidents, particularly as they relate to any compromised information or the business and scope of company operations;
- The range of harm that cybersecurity incidents could cause, including harm to a company's reputation, financial performance, and customer and vendor relationships; and
- The possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities.

As to timing, the Guidance recognizes that a victim company's cooperation with law enforcement to investigate a cyberattack might impact the scope and timing of disclosures, but warns that "an ongoing internal or external investigation—which often can be lengthy—would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident." Notably, the Guidance reminds companies of their duty to correct and duty to update prior disclosures or omissions in light of facts learned through an investigation of a cyberattack.

At a more granular level, the Guidance suggests that companies consider the impact of cybersecurity risks and incidents in reporting risk factors, MD&A, description of the business and legal proceedings pursuant to Regulation S-K and on Form 20-F, in financial statement disclosures, and when describing the board's role in risk oversight.

The second half of the Guidance addresses three additional topics: (1) adoption and regular assessment of disclosure controls and procedures; (2) ensuring that policies and procedures are in place to address the risk of insider trading based on material non-public cybersecurity risks or incidents; and (3) ensuring compliance with Regulation FD when disclosing cybersecurity risks and incidents. Debevoise will shortly publish an additional update with further thoughts on those portions of the Guidance.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Matthew E. Kaplan
mekaplan@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Paul M. Rodel
pmrodel@debevoise.com

Steven J. Slutzky
sjslutzky@debevoise.com

Joshua M. Samit
jmsamit@debevoise.com

Sandeep S. Dhaliwal
ssdhaliwal@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com