BNA Privacy Law Watch

December 30, 2011

Cybersecurity

Whether Cyber-Incident Poses 'Material Risk' Needing SEC Disclosure Is Tough Question

by Katie W. Johnson

In light of recent Securities and Exchange Commission cybersecurity disclosure guidance, publicly traded companies should begin a dialogue with each other about the multiple disclosures they may need to make to the SEC in the event of a cyber-threat or data breach incident, Olga Khvatskaya, counsel in Hunton & Williams LLP's New York City office, said Dec. 14.

However, the question of whether such information is "material"—the trigger in the guidance on when the SEC recommended that a disclosure should be made— is unclear, Khvatskaya said during a webinar hosted by the law firm.

Although there are no existing cybersecurity incident or data breach disclosure requirements for public companies registering with the SEC, the SEC Division of Corporation Finance's nonbinding guidance on cybersecurity disclosure obligations recommended that firms disclose data security compromises because they impact other matters, such as a firm's current and future financial condition (200 PRA, 10/17/11).

The speakers at the webinar "Cybersecurity: SEC Guidance, Disclosure Considerations and Planning for the Unexpected," all of Hunton & Williams, also included Allen Goolsby, special counsel, Richmond, Va.; David Lashway, partner, Washington; Lisa Sotto, partner, New York City; and John Woods, partner, Washington.

In Cyberspace, What Are 'Material' Risks?

Under federal securities laws, the nondisclosure of a material fact could result in liability, Khvatskaya said.

While the SEC guidance defines material information, there is no bright-line test on whether a cybersecurity event or risk is material, she said, explaining that such a determination involves a facts and circumstances analysis.

For example, in the event of a hacking incident, firms may wish to consider:

- the incident's magnitude;
- the nature of the business;
- the type of data subject to the hacking;
- the company's liability and reputation; and
- the incident's impact on contractual provisions, business opportunities and relationships, financial statements and guidance, and internal controls.

One difficulty in a materiality determination, she said, is the uncertainty about whether an incident occurred, its scope, and its consequences.

While the SEC guidance defines material information, there is no bright-line test on whether a cybersecurity event or risk is material.Another stumbling block is the timing of the disclosure. "The more time you have for the analysis, the more accurate disclosure you're probably going to be able to prepare," Khvatskaya said. "But in a lot of these circumstances, you don't have a lot of time."

For example, if a cybersecurity incident occurs immediately before a deadline for a quarterly or annual disclosure, a company may not have a lot of time to analyze the event. In many circumstances, a firm must file with the SEC a Form 8-K, which discloses key corporate information that could be of interest to shareholders.

Khvatskaya recommended that firms make their cybersecurity communications to the SEC consistent with their Regulation FD (Fair Disclosure) policy. Under Regulation FD—which she described as a "hot button issue" not mentioned in the guidance—public companies must disclose material information to all investors simultaneously.

A material cybersecurity incident may also trigger a firm's duty to disclose. She said that a firm should think about the fairness of the disclosure, or it may have "an informational advantage over the public at large."

If a company makes an earnings call or issues guidance, Khvatskaya said that it should be truthful, because what it says may be challenged.

Disclosure Challenges

Khvatskaya emphasized that a discussion of cyber incident risk factors—which the SEC guidance recommends disclosing—should be tailored to a company's business.

Making fact-specific disclosures poses many challenges, she said. For example, in the case of an actual incident, a company may be reluctant to describe an event that is not yet fully understood by the company.

The main issue, Khvatskaya said, is making a "meaningful and not boilerplate disclosure yet not so narrow that it could be challenged on factual grounds."

She noted that forward-looking disclosures may be difficult, such as the guidance's recommendation to address in a Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A) a cybersecurity risk or incident that "would cause reported financial information not to be necessarily indicative of future operating results or financial condition."

Khvatskaya emphasized that the guidance's suggestion to disclose "material" legal proceedings in Forms 10-Q and 10-K includes "contingencies" like "warranty exposure, breach of contract liability, product recall and replacement, and indemnification of third parties."

Companies will also have to comply with accounting rules, she said, noting that a firm may have to disclose a material incident that occurs after the close of a reportable quarter but before the periodic report's publication.

Although Form 8-K does not contain a specific line item for material cybersecurity risks and events, she said that such a risk or event could trigger other line items. For instance, a company may have to disclose a cybersecurity risk or event if it interrupts employees' ability to trade in their 401(k) accounts but permits insiders to continue trading.

"Disclosure is the prism through which you look at factual circumstances," Khvatskaya said.