PRESENTED AT

Essential Cybersecurity Law

July 25, 2018
Houston, TX

Civil Litigation and Regulatory Update

Mark L. Krotoski

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Key Aspects Of SEC Guidance On Cybersecurity Disclosures

By **Mark Krotoski and Kurt Oldenburg** (March 2, 2018, 12:28 PM EST)

Mark Krotoski

Kurt Oldenburg

The U.S. Securities and Exchange Commission on Feb. 21 voted unanimously to approve its commission statement and guidance on public company cybersecurity disclosures. The guidance highlights the need for cybersecurity disclosures based on current reporting obligations and the materiality standard, identifies specific cybersecurity risk factors, and emphasizes two new areas of focus concerning the adoption by public companies of appropriate policies and procedures to address cybersecurity matters and to enforce insider trading prohibitions.

In the guidance, the SEC concluded that, based on "the increasing significance of cybersecurity incidents," it was "necessary to provide further Commission guidance" on cybersecurity disclosures and related issues.[1] As an SEC interpretation,[2] the guidance carries the highest level of authority and "reinforce[es] and expand[s] upon" the prior staff guidance that the SEC staff issued in October 2011.

This article discusses some of the key components contained in the new guidance.

Cybersecurity Disclosures Based on Reporting Obligations

The guidance notes that while current "disclosure requirements do not specifically refer to cybersecurity risks and incidents," the "obligation to disclose such risks and incidents" arises out of "a number of" requirements based on "a company's particular circumstances."[3] This includes, for example, disclosures in periodic reports such as the annual Form 10-K, including within the "management's discussion and analysis" section, and other areas. The guidance surveys many of the reporting requirements that may obligate companies to address cybersecurity risks and incidents in meeting these obligations.

Cybersecurity Disclosures Under the Materiality Standard

Under the guidance, the materiality standard may trigger disclosure obligations related to cybersecurity risks and incidents.[4] Rather than implementing one standard specific to cybersecurity, the materiality determination remains a fact-specific inquiry. The guidance notes that the "materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations." A careful assessment and analysis requires that the disclosure is "tailored" to the company's "particular cybersecurity risks and incidents."[5]

A variety of factors weigh on this assessment. It includes "the range of harm that such incidents could cause" to a company's "reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-US authorities."[6]

In disclosing material cybersecurity risks and incidents, the guidance makes clear that companies are not required to "make detailed disclosures that could compromise its cybersecurity efforts — for example, by providing a 'roadmap' for those who seek to penetrate a company's security protections." The disclosure should not provide information that would make company "systems, networks, and devices more susceptible to a cybersecurity incident."[7]

Timing of Disclosure

The timing of cybersecurity incident disclosure is a critical balance between a company's desire to provide swift disclosure and the importance of ensuring that the essential facts are understood and the disclosed information is accurate. Depending on the nature of the cybersecurity incident, some reasonable amount of time may be required to determine its scope.

The guidance "recognize[s] that a company may require time to discern the implications of a cybersecurity incident."[8] Disclosure also may be affected by requests from law enforcement to cooperate with an ongoing investigation. In considering the timing issue, the guidance observes that "an ongoing internal or external investigation" cannot "provide a basis for avoiding disclosures of a material cybersecurity incident."[9]

Notably, the guidance makes clear that companies "have a duty to correct" disclosures that are determined later to have been untrue when originally made and may have "a duty to update" disclosures that were correct when made based on later material information, such as when reasonable investors are still relying on such disclosure.[10] In particular, "[c]ompanies should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident."[11]

Cybersecurity Risk Factors

With regard to the disclosure of cybersecurity risks,[12] the guidance identifies several factors to be considered. Some factors, illustratively, include the following:

- Occurrence of prior cybersecurity incidents;
- Probability of future occurrences and their consequences;
- Adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs;
- Aspects of the company's business and operations that give rise to material cybersecurity risks, and the potential costs and consequences of such risks;
- Potential for reputational harm;
- Existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity, and the associated costs;
- Litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.[13]

As noted in the first bullet above, the guidance states that prior or ongoing cybersecurity incidents need to be considered. For example, it may be necessary "to discuss the occurrence of that [prior] cybersecurity incident and its consequences as part of a broader discussion of the types of potential cybersecurity incidents that pose particular risks to the company's business and operations."[14] The guidance notes also that other relevant factors when crafting risk factor disclosure may include "[p]ast incidents involving suppliers, customers, competitors, and others."[15]

Management's Discussion and Analysis of Financial Condition and Results of Operations

Cybersecurity disclosures may be required as part of the management's discussion and analysis of financial conditions, changes in financial condition, and results of operations.[16] As the guidance notes, this may include "the cost of ongoing cybersecurity efforts (including enhancements to existing efforts), the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents, among other matters."[17]

The Role of the Board

Title search: Civil Litigation and Regulatory Update

Also available as part of the eCourse
2018 Essential Cybersecurity Law eConference

First appeared as part of the conference materials for the
2018 Essential Cybersecurity Law session
"Civil Litigation and Regulatory Update"