SEC RELEASES UPDATED PUBLIC COMPANY CYBERSECURITY DISCLOSURE GUIDANCE

Date: 11 April 2018

U.S. Complex Commercial Litigation and Disputes / Investigations, Enforcement and White Collar Alert

By: Steven L. Caponi

On February 21, 2018, the U.S. Securities and Exchange Commission (SEC) released a “Commission Statement and Guidance on Public Company Cybersecurity Disclosures” to help public companies understand their obligations to disclose cybersecurity risks and incidents. According to SEC Chair Jay Clayton, the new guidance interpretation “reinforces and expands” the SEC Division of Corporation Finance's 2011 “CF Disclosure Guidance: Topic No. 2 ─ Cybersecurity.”

While the SEC's new guidance confirms that the 2011 guidance remains valid and repeats and amplifies many of its ideas, the new guidance adds two significant topics for consideration. Specifically, the new guidance (i) discusses the importance of maintaining robust cybersecurity policies and procedures to ensure a company's ability to make accurate and timely disclosures, and (ii) makes clear that trading by company personnel ahead of the disclosure of a cybersecurity incident can constitute illegal insider trading for which public companies should adopt safeguards. It is safe to assume these areas of concern will be focuses of SEC scrutiny going forward, and they provide important clues about the circumstances under which the SEC might bring enforcement actions. Therefore, public companies would be wise to carefully review their cybersecurity policies, procedures, and disclosures to ensure compliance with the new guidance.

Disclosure Controls and Procedures: The new guidance points out that certain rules under the Securities Exchange Act of 1934 require (i) public companies to maintain disclosure controls and procedures, (ii) management to evaluate the effectiveness of those controls and procedures, and (iii) certifications by a company's principal executive and principal financial officers regarding the design and effectiveness of those controls and procedures. The new guidance emphasizes that timeliness in discovering material information is critical to effective disclosure. Accordingly, the new guidance suggests that:

> companies should consider whether such controls and procedures will appropriately record, process, summarize, and report the information related to cybersecurity risks and incidents that is required to be disclosed in filings. Controls and procedures should enable companies to identify cybersecurity risks and incidents, assess and analyze their impact on a company’s business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents.

©2005-2026 K&L Gates LLP. All Rights Reserved.

Through this discussion, the SEC is arguing that if a company does not have robust cybersecurity policies and procedures, it may not learn of and disclose material information as required and, therefore, that cybersecurity is essential to a company's ability to make required disclosures. This linkage between cybersecurity and disclosure gives boards of directors an enhanced oversight obligation to ensure that management has policies and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel so that senior management can make disclosure decisions and certifications in a timely manner. This includes an obligation not only to disclose current cybersecurity events but to update prior disclosures to ensure they remain accurate and complete.

Through the new guidance, the SEC is strongly urging companies to adopt comprehensive cybersecurity policies and procedures and to assess their compliance regularly. Importantly, the new guidance requires that, following a cyber incident, organizations should “disclose the extent of its board of directors' role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board's leadership structure.” This language significantly increases the pressure on boards to engage with the C-suite to ensure cyber risks are managed effectively.

The SEC's new guidance provides examples of factors boards should consider when evaluating their cybersecurity risk disclosures: (i) the occurrence of prior cybersecurity incidents, including their severity and frequency; (ii) the aspects of the company's business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks; (iii) the costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers; and (iv) existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs to companies.

The SEC has clearly elevated cybersecurity risks to the status of a required disclosure when material. However, given the broad definition of materiality and the wide-ranging impact of cybersecurity events, practically speaking, there is likely to be a low threshold to disclosure of some sort. When considering the materiality of an event, companies should consider the potential harm a given cybersecurity risk or incident could cause. This includes the impact on reputational harm, financial performance, customer and vendor relationships, litigation, and regulatory investigations or actions by state and federal agencies.

Insider Trading: Adding teeth to the 2011 guidance and enhanced disclosure requirements, the new guidance contemplates the adoption of policies to prevent trading in company securities when insiders are aware of material nonpublic information related to a cyber incident. While the general warning not to trade ahead of bad news is not novel, the SEC was clear in noting that, when a public company has uncovered a cybersecurity incident or risk that would be material to investors, it must make appropriate and timely disclosure of such items sufficiently prior to any offer or sale of securities. Additionally, the company must take suitable steps to prevent officers, directors, and other insiders from trading in the company's securities until appropriate public disclosure has been made. Again, tying this guidance to disclosure creates another element of pressure to urge companies to report cyber incidents publicly and quickly; in this case, it is the pressure to avoid the possibility of insider trading by company personnel.

The SEC has stated in the 2018 guidance that companies should consider “the ramifications of directors, officers, and other corporate insiders trading in advance of disclosures regarding cyber incidents that prove to be material.” By addressing the ability of insiders to trade in securities when facing a cyber incident or when aware of

©2005-2026 K&L Gates LLP. All Rights Reserved.

material nonpublic cybersecurity risks, the SEC is clearly seeking to put teeth behind its enhanced disclosure requirements. The new guidance will most likely result in a trading “blackout” until such time as the public is informed of all material cybersecurity risks. In turn, these blackouts will place added urgency on companies to ensure they timely disclose all known cybersecurity risks and update prior disclosures so they remain current and accurate.

KEY CONTACTS



STEVEN L. CAPONI
PARTNER

WILMINGTON
+1.302.416.7080
STEVEN.CAPONI@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.