SEC Issues New Cybersecurity Guidance

March 7, 2018 – The TMCA
by Cam C. Hoang and Imeabasi Ibok

On February 26, in the wake of significant and far-reaching cybersecurity breaches (*e.g.*, the Equifax Data Breach), the SEC published interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents. The SEC recognizes that cybersecurity threats present an "ongoing risk" to all public companies which can lead to "substantial costs and other negative consequences" including liability for stolen assets or information and repairs of system damage; increased cybersecurity protection costs, litigation and legal risks; increased insurance premiums; and damage to the company's reputation, competitiveness, stock price and long-term shareholder value.

The SEC's new guidance reinforces and expands on its October 2011 guidance, emphasizing the importance of adopting sound cybersecurity policies and procedures and safeguards against insider trading in the event of a potentially material cybersecurity breach.

Public Disclosure Requirements

The SEC provides that "although no existing disclosure requirement explicitly refers to cybersecurity," periodic reports, current reports and Securities Act and Exchange Act obligations all require public companies to disclose material risks and incidents including those related to cybersecurity. The SEC encourages companies to continue to use current report Form 8-K or Form 6-K to disclose material cybersecurity-related information promptly as this practice reduces the risk of selective disclosure.

Beyond requirements explicitly found in SEC regulations, companies are also required to disclose material information and revisit previous disclosure, especially during a cybersecurity investigation, as may be necessary to ensure the company's filings are not misleading. Notably, companies "have a duty to correct prior disclosures that the

Related People

- Cam C. Hoang

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

company determines were untrue at the time it was made, or a duty to update a disclosure that becomes materially inaccurate after it is made."

The obligation to update prior disclosure is the subject of some debate, and perhaps will merit further guidance from the SEC. According to a footnote in the guidance, the SEC bases this duty to update in *Backman v. Polaroid Corp.*, 910 F.2d 10 (1st Cir. 1990), but acknowledges that other circuits have not found a duty to update. Furthermore, the Private Securities Litigation Reform Act expressly disclaims any duty to update forward-looking statements. 15 U.S.C. §§ 77z-2(d) and 78u-5(d) ("Nothing in this section shall impose upon any person a duty to update a forward-looking statement."). A duty to update prior disclosure, and the associated work and potential liability, may constrain future disclosure of cybersecurity risk.

The SEC provides the following examples of factors companies should consider when evaluating their cybersecurity risk disclosure: 1) the occurrence of prior cybersecurity incidents, including their severity and frequency; 2) 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; 3) the costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers; and 4) 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 cautions that this guidance is not intended to suggest that a company should make detailed disclosures that could compromise its cybersecurity efforts. There is no general requirement to expose potential system vulnerabilities in such a way that would make the company more susceptible to risk. However, the SEC expects that companies will provide disclosure that is tailored to their particular cybersecurity risks and incidents using company-specific, useful information as opposed to boilerplate language.

The SEC guidance suggests companies adopt comprehensive policies and procedures related to cybersecurity and assess their compliance regularly. Companies should have adequate disclosure controls and procedures in place to ensure that relevant cybersecurity information is processed and reported to the appropriate personnel to enable senior management to make disclosure decisions and certifications. These policies will not only allow the company to adhere to the SEC's disclosure requirements but will also facilitate policies and procedures designed to prohibit directors, officers, and other corporate insiders from trading on the basis of material nonpublic information about cybersecurity risks and incidents.

Insider Trading

The SEC guidance provides that companies and their corporate insiders should be mindful to adhere to the federal antifraud provisions as well as other applicable rules (such as codes of conduct required by exchanges) related to insider trading in connection with information about cybersecurity risks and incidents. The SEC guidance advises companies in the midst of investigating significant cybersecurity incidents to

consider implementing restrictions on insider trading in their securities to prevent corporate insiders from trading on the basis of material nonpublic information before the incident has been publicly disclosed, and to avoid the appearance of improper trading.

Conclusion

Companies are facing rapidly evolving cybersecurity threats. It is increasingly important for companies to investigate and refine their own disclosure policies and procedures to ensure a momentary lapse in cybersecurity judgment does not culminate in unnecessary damages to the company or SEC enforcement actions. The new SEC cybersecurity guidance can be found in its entirety here.