Published on *The National Law Review* https://natlawreview.com

February 26, 2018 - Privacy and Cybersecurity Group News: SEC Issues New Cybersecurity Disclosure Guidance for Public Companies

Article By:

Edward B. Whittemore

On February 21, 2018, the SEC approved new interpretive guidance to assist public companies in preparing their disclosures about cybersecurity risks and incidents. The Release builds upon and expands on the SEC's 2011 staff guidance on cybersecurity matters.

In the Commission's release, the SEC explained that it:

- believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack.
- expects companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences.
- believes that companies are well served by considering the ramifications of directors, officers, and other corporate insiders trading in advance of disclosures regarding cyber incidents that prove to be material.
- expects companies, in their management discussion & analysis sections of their public filings addressing their results of operations and financial condition, to consider an array of potential costs that may be associated with cybersecurity issues, including: remediation costs, such as liability for stolen assets or information, repairs of system damage, increased cybersecurity protection costs, lost revenues resulting from the unauthorized use of proprietary information or the failure to retain or attract customers following an attack; litigation and legal risks, including regulatory actions by state and federal governmental authorities and non-U.S. authorities; increased insurance premiums; reputational damage that adversely affects customer or investor confidence; and damage to the company's competitiveness, stock price, and long-term shareholder value.

The SEC also reminded public companies of the ways in which cybsersecurity incidents, and their related costs, can impact a company's financial statements, its disclosure controls and procedures, and insider trading compliance program. The SEC Release also specifically addresses the importance of company disclosure to investors about how the company's board of directors is discharging its risk oversight responsibility with respect to the company's cybersecurity risk management policies and procedures.

The SEC's February 21st release is here: https://www.sec.gov/rules/interp/2018/33-10459.pdf

The statement of Commissioner Clayton is here: https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21

National Law Review, Volume VIII, Number 58