wiley

ALERT

SEC Expands Guidance on Cybersecurity Disclosure Obligations

February 22, 2018

On February 21, 2018, the Securities and Exchange Commission (SEC) announced much-anticipated guidance which updates previous guidance on disclosing cybersecurity risk. The Commission stated it was "reinforcing and expanding upon the staff's 2011 guidance," while continuing to consider other means of promoting appropriate disclosure of cyber incidents.

One takeaway from this guidance is that some uncertainty will remain as to what is material. That said, the SEC is sending clear signals. Companies must pay more attention to the quality and nature of their disclosures and Board management is top of mind at the Commission. Companies should double down on efforts to ensure they have solid policies and procedures, and consider SEC risk when handling a cyber incident.

This update comes against the backdrop of other executive branch activity on market transparency and disclosure in response to President Trump's 2017 Executive Order, as well as statements by senior government officials signaling increasing expectations about private sector efforts on cybersecurity. The government is also looking at measurement and metrics for cyber risk management, in other venues. Stay tuned for more developments.

What did the SEC say?

Like the previous guidance from 2011, the Commission stated that companies must inform investors about "material cybersecurity risks and incidents in a timely fashion." While materiality is still the lynchpin of any disclosure, the Commission's new guidance significantly expands on what it expects from companies, including, in

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kevin B. Muhlendorf
Partner
202.719.7052
kmuhlendorf@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

Securities Enforcement and Litigation

some instances, additional information about how the Board manages cyber risk as well as information about past cyber incidents. Further, the Commission emphasized the critical role a company's cybersecurity policies and procedures play in identifying and managing cyber risk. Lastly, the Commission emphasized that corporate insiders may be prohibited from trading on non-public material information related to cyber risk.

The SEC Offers Some Clarification of Materiality. The Commission provided additional clarification on when a cyber risk may be material to investors. The Commission stated that materiality may depend on the "nature, extent, and potential magnitude" of cyber incidents, and may depend on "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."

The Commission listed the following factors to consider in determining cybersecurity risk factor disclosure:

- the occurrence of prior cybersecurity incidents, including their severity and frequency;
- the probability of the occurrence and potential magnitude of cybersecurity incidents;
- the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the company's ability to prevent or mitigate certain cybersecurity risks;
- 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, including industry-specific risks and third party supplier and service provider risks;
- the costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers;
- the 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 to companies; and
- litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.

The Commission cautioned companies against boilerplate disclosure language. Instead, the Commission emphasized that cyber risks should be "tailored" to each individual company and should "provide specific information that is useful to investors."

However, the SEC Reminds Companies that Disclosure Should Not Compromise Security. Like the 2011 Guidance, the Commission emphasized that cyber risk disclosures should not be so detailed as to compromise cybersecurity efforts, by, for example, providing a "roadmap" to nefarious hackers. The Commission added that, "[w]e do not expect companies to publicly disclose specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident." Despite the Commission's recognition of the harm of detailed cyber risk disclosures, it will remain a challenge for companies to provide information that is sufficiently specific and tailored while avoiding creating a

vulnerability by disclosing cyber risks to the general public.

There is a Heightened Focus on Cyber Policies and Procedures. The Commission made it clear that companies must have actionable cybersecurity policies and procedures. The Commission stated, "[c]ybersecurity risk management policies and procedures are key elements of enterprise-wide risk management . . . We encourage companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure." The Commission expressly contemplates that SOX certifications should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents.

Disclosures Should Describe How the Board Handles Cyber Risk. The Commission stated that, "[a] company must include a description of how the Board administers its risk oversight function," which should include a discussion of the Board's role in overseeing the management of any material cyber risk. The Commission believes that disclosures about a company's cyber risk management program and insight into how the Board discharges its cyber risk oversight responsibility may be important to investors' assessments of a company.

Caution: Companies May Need to Disclose Past Cyber Incidents. The Commission stated that in order to provide appropriate context of a company's cyber risks, it may be necessary to disclose previous cyber incidents. For example, the Commission stated that if a company experiences "a material cybersecurity incident" involving a denial of service attack, disclosure of that incident may be necessary to properly inform investors about the risk of future denial of service attacks. Further, going beyond a company's own cyber incidents, the Commission stated that past incidents involving "suppliers, customers, competitors, and others" may be relevant when crafting risk factor disclosure.

Reminder: Insider Trading is Prohibited. Lastly, the Commission noted that in some instances insider trading prohibitions may be applicable in the cyber context. Specifically, the Commission stated that cybersecurity risk and incidents may be "material nonpublic information," and corporate insiders would be prohibited from trading while in possession of that information. The Commission further reminded issuers that in addition to evaluating their exchange mandated codes of ethics and insider trading policies to make sure they address any trading based on cybersecurity issues, they should also be mindful of selective disclosures of cybersecurity incidents which would violate Regulation FD. The Commission expects companies to have polices in place to comply with Regulation FD, which now explicitly includes cybersecurity related disclosures.

To Wrap Up...

The Commission's increased expectations for expanded disclosure of cyber risk underscores the importance of managing cyber risk on an enterprise level. Companies must carefully examine every aspect of how they handle cyber risk and be prepared to defend those decisions in a public setting. As the Commission's guidance indicates, companies can expect increased scrutiny on their cyber policies and procedures, the Board's role in overseeing cyber risk, and the handling and resolution of past cyber incidents.

***

Wiley Rein's Cybersecurity Practice has been helping clients with these and other issues for years. We draw on a multidisciplinary approach to help major companies and entire industries manage risk, share information, and prepare for and handle incidents. We also handle Congressional and agency investigations in the areas of cyber and data security.