Articles + Publications | February 22, 2018

Locke Lord QuickStudy: Cybersecurity Disclosures: Takeaways From the SEC's New Guidance

WRITTEN BY

Stanley Keller

The New

The new guidance addresses two new issues that the SEC did not address in the previous staff guidance. First, the SEC stresses that cybersecurity risk management policies are key elements of a company's general disclosure controls and procedures.[3] For companies that have not already done so, the SEC strongly encourages them to adopt and maintain comprehensive disclosure controls and procedures that relate to cybersecurity risks. This includes having policies and procedures in place to ensure that timely notifications of cybersecurity incidents are reported up to senior management.

Disclosure and Control Procedures The focus on cybersecurity disclosure and control policies is important in the context of the required certification by a company's CEO and CFO (or principal financial officer) regarding the design and effectiveness of a company's disclosure controls and procedures. These certifications should now take into account the adequacy of the company's cybersecurity disclosure controls and procedures. *Insider Trading Policies* The SEC cautions that a company's undisclosed cybersecurity incident may involve material, nonpublic information that could cause a company's officers, directors and other insiders to violate the antifraud provisions of the Exchange Act if they trade in the company's securities while the cybersecurity incident remains nonpublic information. The SEC encourages companies to consider establishing certain policies, such as restrictions on insider trading following a cybersecurity incident, to avoid the appearance of improper insider trading. This is an especially important caution in view of the recent Equifax hack and the probe surrounding executives' stock sales after the hacking incident. The SEC also reminds companies of the requirements of Regulation FD to avoid selective disclosures of material cybersecurity matters. **The Old** In October 2011, the SEC's Division of Corporation Finance issued interpretive guidance to assist public companies in assessing their disclosure obligations concerning cybersecurity risks and incidents in registration statements and periodic reports. Given the increased risks that cybersecurity poses to companies in nearly every industry now, the SEC has provided an update on its previous guidance. The following chart highlights when existing disclosure requirements may impose an obligation on a company to make certain cybersecurity disclosures. **Regulatory Item** **SEC Guidance**

	• prior cybersecurity incidents, including their severity and frequency • probability of an incident and potential magnitude of the incident • whether the company's business or industry gives rise to material cybersecurity risks • costs associated with cybersecurity protection If a company has experienced a specific cybersecurity incident, it may not be enough to disclose the potential risk of another incident occurring. The company should discuss in further detail the occurrence and its consequences, alongside a broader discussion of cybersecurity risks inherent in the company's business or industry.
Item 303(c) – MD&A of Financial Condition and Results of Operation	Companies should consider the following to determine whether disclosure of cybersecurity risks is necessary: In disclosing information the company's management believes necessary to understanding its financial condition and results of operations, management may want to consider whether the costs of cybersecurity (such as loss of IP, reputational harm, and cybersecurity insurance) and the potential risks and consequences of an incident could further inform management's discussion and analysis. In addition, the SEC expects companies to consider cybersecurity issues and their impact on each of the company's reportable segments.
Item 101 – Description of Business	The SEC expects companies to discuss cybersecurity incidents or risks if it would materially affect a company's products, services, relationships with customers or suppliers, or competitive conditions.
Item 103 – Legal Proceedings	Any litigation arising out of a cybersecurity incident must be properly disclosed. For example, if a company is hacked and all of its customers' information is stolen, the company must disclose any material litigation, including suits brought by the affected customers against the company.

		impact of a cybersecurity incident is reflected on the financial statements in a timely manner. For example, an operational event such as a hack could result in a possible loss contingency requiring financial statement accrual or disclosure.
Item 407(h) Board Risk Oversight	Item 407(h) Board Risk Oversight	A company's risk management and control systems should be discussed so that Board risk oversight can be understood. Companies should include a discussion on the Board's role in overseeing cybersecurity risks.

Takeaways

Given the increased magnitude and frequency of cybersecurity incidents, public companies should revisit their cybersecurity disclosures and disclosure controls and procedures. Despite the criticism by some that the SEC's new guidance does not go far enough,[4] that guidance should serve as a wake-up call for companies that have not yet put in place a comprehensive cybersecurity disclosure policy. A public company without such a policy is urged to put one in place so that it is in a position to timely report and to alert investors of any data breaches or other cybersecurity incidents. Those public companies that have a cybersecurity disclosure policy in place should review and update that policy, having in mind that cybersecurity incidents are becoming more and more common and that increased attention by the SEC and others on cybersecurity disclosure is assured. In addition to disclosure and governance considerations, companies should continue to treat the subject of cybersecurity as a critical operational issue deserving of focused attention.

1 SEC Rel. Nos. 33-10459; 34-82746, located here.

2 CF Disclosure Guidance Topic No. 2, Cybersecurity located here

3 Public companies are required to maintain effective disclosure controls and procedures pursuant to Exchange Act Rules 13a-15 and 15d-15.

4 https://www.law360.com/articles/1014661/new-sec-cybersecurity-guidance-dinged-by-dems-as-rehash

RELATED INDUSTRIES + PRACTICES

- Capital Markets