orrick
Trust Anchor

SEC Commissioners Provide Guidance on Cybersecurity Disclosures After Wave of Record Incidents

Editorial Board (https://blogs.orrick.com/trustanchor/author/editorialboard/)

Much has been written about the SEC's **interpretive guidance on cybersecurity disclosures** (https://www.sec.gov/news/press-release/2018-22), issued in late February, including **Commissioner Stein's statement** (https://www.sec.gov/news/public-statement/statement-stein-2018-02-21)that it *under*-delivers for investors, public companies, and the capital markets. As many **observers have noted** (https://www.sec.gov/news/public-statement/statement-jackson-2018-02-21), the Commission largely repackaged the Division of Corporation Finance's prior **October 2011 guidance** (https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm). Further, by issuing interpretive guidance, rather than engaging in formal rulemaking, the SEC's pronouncement does not have the force and effect of law and is not accorded such weight in the adjudicatory process.[1]

From an overview perspective, the Commission's guidance simply reminds us that digital technologies can create enterprise risk; that the securities laws mandate disclosures of material risk; that disclosure controls and procedures are critical and more effective when directors and officers are involved; and that trading on material nonpublic information is prohibited. These are hardly new concepts. Indeed, the general nature of these pronouncements is the source of frustration for those seeking more specific and potentially proscriptive direction.[2]

The Commission, however, chose its topics and words carefully; and close analysis reveals valuable details and insights. Thus, in addition to summarizing what the guidance "says," we offer a closer look at what the guidance "means" in terms of immediate action items for publicly traded entities and practitioners.

What Is in the New 2018 Guidance?

Duty to Disclose. The Guidance indicates that including risk of cybersecurity incidents within corporate disclosures of risk factors—a practice that became commonplace after the 2011 guidance—is not enough. Instead, "[c]ompanies must provide timely and ongoing information in [] periodic reports regarding material cybersecurity risks and incidents that trigger disclosure obligations."

In essence, the SEC's position is that companies cannot stay silent and have a duty to disclose material nonpublic information relating to cybersecurity risks and incidents.[3] This position is broader than established Supreme Court precedent, which provides that disclosure is mandated only if a company is trading on the information, a statement or omission would render a prior statement materially misleading, or disclosure is expressly required.

In the context of the duty to update and correct prior disclosures, the Guidance provides that a company cannot rely on an ongoing internal or external investigation of a cybersecurity incident to withhold information as that "would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident." Moreover, companies "may have a duty to correct [a] prior disclosure that the company determines was untrue . . . or a duty to update [a] disclosure that becomes materially inaccurate after it is made."

The materiality of cybersecurity risks or incidents "depend[s] upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations." The Guidance indicates that materiality analysis for cybersecurity should include (1) remediation costs; (2) increased cybersecurity protection costs; (3) lost revenues; (4) litigation and legal risks; (5) increased insurance premiums; and (6) reputational damage, including potential negative impact on the company's stock price.

Disclosure Controls and Procedures. The Guidance stresses the importance of adopting and maintaining disclosure controls and procedures that will ensure relevant information about cybersecurity risks and incidents is timely processed and reported to appropriate personnel all the way up to senior management. Before an incident, companies should assess whether their disclosure controls and procedures will enable them to (1) identify cybersecurity risks and incidents; (2) assess and analyze the impact of such risks and incidents on the company operations, including on each reportable segment; and (3) evaluate the potential materiality of such risks and incidents. Additionally, policies should provide for open communications between technical experts and disclosure advisors regarding such risks and incidents. In making Sarbanes-Oxley Act 302 certifications per Exchange Act Rules 13a-14 and 15d-14 for quarterly and annual reports regarding the design and effectiveness of disclosure control and procedures, a company's principal executive officer and principal financial officer should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents. If cybersecurity risks or incidents pose a risk to a company's ability to record, process, summarize and report information required to be disclosed in SEC filings, management should consider whether disclosure controls and procedures are effective.

Special Emphasis on Service Providers. In multiple places throughout the guidance, the Commission mentions third-party "suppliers," "service providers," and "vendors" as critical to, among other things, enterprise risk, cyber incidents, and response and remediation costs. Thus, the guidance admonishes companies to think long and hard about service providers in providing contextual disclosures (e.g., "Past incidents involving suppliers, customers, competitors, and others may be relevant when crafting risk factor disclosure.").

Public research confirms that vendor-attributed data breaches are exceedingly common. In one oft-cited study, Soha Systems found that **63 percent of data breaches may be directly or indirectly related to third-party access** (https://static1.squarespace.com/static/56b3cadb59827ecd82b02b43/t/5906176a893fc052557a0646/1493571436523/Soha_Systems_Third_Party_Advisory_Group_2016_IT_Survey_Report.pdf) by contractors and suppliers. Widespread migration to cloud services, and outsourcing more generally, portends even greater potential for risk exposure—particularly for entities engaged in financial services, health care, and other sectors that have experienced serious data breaches in recent years.

The foregoing makes clear that companies should consider how their disclosures might be affected by operational connectivity (and sometimes, integration) with various third parties. Where companies rely on third parties not only for operational support but also for security controls, careful thought should be given as to how risk is disclosed. Specifically, risk disclosures may need to account for the fact that failures in a critical vendor's security measures to protect against, identify, detect, or respond to major cyber events could materially impact the company itself.

Insider Trading Policies and Blackout Periods. The Guidance encourages companies to review their code of ethics and insider trading policies to assess whether they take into account cybersecurity incidents. Additionally, the Guidance indicates that it may be appropriate to implement a trading blackout period while the company investigates and assesses the significance of a cybersecurity incident. Implementing a blackout period following an incident and prior to disclosure could protect against insider trading and avoid the appearance of improper trading during this period.

Regulation FD and Selective Disclosure. The Guidance reminds companies that persons acting on behalf of a company should not selectively disclose material nonpublic information relating to cybersecurity risks and incidents to brokers, dealers, investment advisors, and other persons enumerated in Regulation FD before disclosing the same information to the public. Companies should adopt policies and procedures to avoid selective disclosure prohibited by Regulation FD, or ensure a Form 8-K disclosure is made where such information is provided to Regulation FD enumerated persons, which may occur when a company is required to provide notification to individuals under state data breach notification requirements or other regulatory requirements.

Risk Committee and Board Oversight. Disclosure in annual reports or proxy statements of the board of directors' role in risk oversight of a company pursuant to Item 407(h) of Regulation S-K should include a discussion of the nature of the board's role in overseeing the management of cybersecurity risks that are material to a company's business. In addition, disclosures on how the board engages with management on cybersecurity issues will allow investors to assess how a board of directors is discharging its risk oversight responsibility in cybersecurity matters.

What Should Companies Do to Comply With the New Guidance?

In light of the SEC's new Guidance on cybersecurity, companies should consider the following:

- Identify and scrutinize all prior disclosures about cybersecurity and consider whether previous disclosures need to be revisited, updated or corrected, including during the process of investigating

a cybersecurity incident (which should be specifically articulated in the company's incident response plan).

- Review disclosure controls and procedures to determine if incidents and breaches are, or can be, timely escalated to senior management and legal department for disclosure analysis and certifications.
- Assess whether disclosure controls and procedures provide a method to determine the impacts of cybersecurity risks and incidents on the company and a protocol to assess the potential materiality of such risks and incidents.
- Review disclosure controls and procedures to assess whether procedures are in place to determine whether implementing a blackout period while the company investigates and assesses the significance of a cybersecurity incident is appropriate, and review insider trading policies to ensure they prohibit insiders from trading in company securities when in possession of material nonpublic information relating to cybersecurity risks and incidents.
- Review the company's incident response plan to determine if the appropriate level of coordination between information security, communications, legal, and management is included and that policies, procedures, and structures are in place for open communication between technical experts and disclosure advisors when an incident has occurred to protect against misstatements.
- Assess the company's Regulation FD policy to ensure that any disclosures of material nonpublic information related to cybersecurity risks and incidents are not made selectively, and that Form 8-K disclosure is made simultaneously if material nonpublic information is provided to those persons enumerated in Regulation FD in connection with state data breach notification requirements.
- In preparing annual and quarterly reports and registration statements,
    - Avoid generic risk factors relating to cybersecurity and instead tailor them to the company's actual threat landscape, which could include some or all of the eight factors contained in the Guidance;
    - When crafting MD&A disclosure regarding events, trends, and uncertainties that are reasonably likely to have a material effect on results of operations, liquidity, or financial condition, consider the costs of ongoing cybersecurity efforts, the costs and other consequences of cybersecurity incidents, including the impact on reportable segments, and the risks of potential cybersecurity incidents; and
    - Make sure the range and magnitude of financial impacts of a cybersecurity incident, as they become available, are incorporated into financial statements on a timely basis.

---

[1] The SEC initially indicated that it was poised to tackle the issue by issuing a Sunshine Act Meeting notice on February 14, 2018, for a meeting on February 21, 2018. The purpose of the meeting was to discuss cybersecurity, and specifically "whether to approve the issuance of an interpretive release to provide guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents." However, the meeting was unceremoniously cancelled the day before it was to occur. Instead, the SEC issued its cybersecurity guidance via seriatim.

[2] As Commissioner Stein noted in her statement about the new guidance: "To be sure, these are all valuable reminders and raising them to the Commission level indicates a level of significance the staff guidance from seven years ago simply does not. The problem, however, is that many of these reminders were offered by the staff back in 2011. . . . The more significant question is whether this rebranded guidance will actually help companies provide investors with comprehensive, particularized, and meaningful disclosure about cybersecurity risks and incidents. I fear it will not."

[3] Although the SEC acknowledged that none of its regulations "specifically refer[s] to cybersecurity risks and incidents," it insists that "an obligation to disclose such risks and incidents" is imposed by a "number of requirements," such as periodic reporting requirements or Securities Act and Exchange Act requirements. What is required will "depend[] on the company's particular circumstances." For example, "companies may need to disclose previous or ongoing cybersecurity incidents or other past events in order to place discussion of [cybersecurity] risks in the appropriate context." The suggestion that "[t]his type of contextual disclosure may be necessary to effectively communicate cybersecurity risks to investors" was foreshadowed by the SEC in its **amicus brief** (http://www.scotusblog.com/wp-content/uploads/2017/09/16-581-bsac-unitedstates.pdf) to the Supreme Court in *Leidos, Inc. v. Indiana Public Retirement System*, relating to Item 303 statements.