ROPES & GRAY ALERT

Securities & Public Companies ▪ Privacy & Cybersecurity

February 28, 2018

SEC Issues New Cybersecurity Disclosure Guidance

On February 21, 2018, in response to the increasing significance of cybersecurity incidents, the Securities and Exchange Commission ("SEC") announced much-anticipated interpretive guidance on cybersecurity disclosure. The guidance affirms and expands upon the 2011 cybersecurity disclosure guidance issued by the staff of the Division of Corporation Finance.[1] The new guidance also notably addresses the importance of the board's role in overseeing the management of cybersecurity risks, the need for corporate cybersecurity policies and procedures, considerations concerning potential insider trading prohibitions by companies investigating potential breaches, and Regulation FD and selective disclosure prohibitions in the cybersecurity context. Overall, the new guidance is consistent with pressure being exerted on companies in all industries by regulators, counterparties and industry bodies to treat cybersecurity as an enterprise-level risk, and to ensure that companies' processes, procedures and disclosures properly consider and address that risk. The text of the SEC's new guidance is available here.

Disclosure Requirements

With the exceptions noted below, the SEC's guidance covers much of the same ground that the staff's 2011 guidance addressed, reminding companies to consider the materiality of cybersecurity issues when preparing required disclosures in SEC filings. Information about cybersecurity and cyber incidents may be required as part of each of the following standard disclosures. However, as we discuss below, given the multiple stakeholders with an interest in any potential incident, disclosure considerations, particularly those relating to an ongoing cyber incident, should be carefully coordinated.

- ***Risk Factors.*** The SEC reiterated that companies should disclose material risks associated with cybersecurity and cybersecurity incidents, including risks that arise in connection with acquisitions. In addition, the SEC noted that companies may need to disclose previous or ongoing cybersecurity incidents or other past events in order to place discussions of risks in the appropriate context.
- ***Management's Discussion and Analysis.*** For MD&A, the guidance provides that companies should address the costs and consequences of cybersecurity risks and cybersecurity incidents, including the costs of ongoing cybersecurity efforts (including enhancements to existing efforts), cybersecurity insurance, and the costs associated with cybersecurity issues, including the loss of intellectual property, regulatory compliance, and remediation costs. The SEC also expects companies to consider the impact of cybersecurity incidents on each of their reportable segments.
- ***Description of Business.*** The SEC requires companies to disclose cybersecurity incidents and risks that materially affect a company's products, services, relationships, or competitive conditions. The SEC acknowledges that any disclosure should not be so robust that it provides a roadmap to breaching the company's systems or products.
- ***Legal Proceedings.*** Disclosure of material pending legal proceedings may require the disclosure of litigation that relates to cybersecurity issues.

[1] *See* CF Disclosure Guidance: Topic No. 2 – Cybersecurity (Oct. 13, 2011), available at https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

- ***Financial Statement Disclosures.*** As part of financial statement disclosures, cybersecurity incidents and the resultant risks may affect a company's financial statements. Disclosures may be required about costs related to investigation, remediation and litigation, possible loss contingencies, diminished future cash flows and impaired assets resulting from a cybersecurity incident.

- ***Board Risk Oversight.*** As a new area of interpretive guidance, the SEC points to the existing requirement that companies disclose the role of the board in risk oversight. The new guidance instructs companies to include specific disclosures about cybersecurity risk management, and how the board of directors engages with management on cybersecurity issues, but only to the extent that cybersecurity risks are material to a company's business. This trend is consistent with calls by institutional investors for better insight into the board's oversight of risk management. However, the implication of this principles-based guidance is that companies need to make specific disclosures of how the board oversees **each** risk it identifies as material.

Disclosure Controls and Procedures

The guidance encourages companies to adopt "comprehensive policies and procedures related to cybersecurity" and to assess their compliance environment regularly. This assessment should include the sufficiency of the company's disclosure controls and procedures relating to cybersecurity risks and incidents. In particular, the new guidance highlights the importance of ensuring that cybersecurity incident response teams are well coordinated with disclosure, compliance and other non-IT professionals within a company. The SEC's guidance cautioned that "an ongoing internal or external investigation – which often can be lengthy – would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident."

The guidance further states that companies should assess whether their disclosure controls and procedures are adequate to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to determine whether disclosure is required. In a sentence that is likely to generate much angst, the SEC states that disclosure controls should ensure timely collection and evaluation of "information potentially subject to required disclosure . . . ." Although this universe of information could be almost limitless, we believe the point being made is that there should be a process in place to evaluate and escalate information involving cybersecurity risks, including information about cybersecurity incidents as they unfold, so that management can appropriately assess materiality and reach timely disclosure decisions. In addition, and perhaps as a reminder that there is individual responsibility as well, the new guidance notes that CEO and CFO certifications that accompany a company's periodic reports should "take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact."

Other Corporate Policies

Insider Trading. The guidance encourages companies to consider how their codes of ethics and insider trading policies take into account and prevent insider trading on the basis of material, non-public information related to cybersecurity risks and incidents. In addition, the guidance asks companies to consider whether and when it may be appropriate to implement insider trading "blackout" periods during the investigation and assessment of material cybersecurity incidents.

Regulation FD. Companies also may have disclosure obligations under Regulation FD in connection with cybersecurity matters. The SEC expects companies to have policies and procedures to ensure that any disclosure of material, non-public information related to cybersecurity risks and incidents is not made selectively, and that any Regulation FD required public disclosure is made in compliance with the rule.

What To Do Now

As noted by Commissioners Stein and Jackson, both of whom issued statements in conjunction with the approval of the guidance, there is not a lot here that is new. Companies that have been carefully following and implementing the

2011 staff guidance should be positioned well to monitor, assess, address and disclose risks related to cybersecurity. There are several things, however, that companies should consider immediately:

- **Review Cybersecurity Governance Structure.** Companies should review generally their governance structures for cybersecurity and enterprise risk management. Managing cybersecurity risk is not the exclusive province of IT professionals. A company's officers, and ultimately its board, should have a thorough understanding of the cybersecurity risks the company faces, how it addresses those risks, and the costs of mitigating those risks. Well-thought-out, enterprise-level cybersecurity risk management programs, as well as incident response and disaster recovery plans that are regularly tested, are important foundations for any company.

- **Review Disclosure Controls and Procedures.** A company's disclosure controls and procedures should be reviewed to ensure that they address how to treat cybersecurity incidents and provide a clear escalation path consistent with a company's incident response plan. Companies should review their existing disclosure controls and procedures and revise them, as appropriate.

- **Enhance Disclosure of Board Risk Oversight in the Proxy Statement.** The guidance suggests that the SEC is looking for specific disclosure of how the board's risk oversight function deals with cybersecurity. Companies preparing this year's proxy disclosure should specifically address cybersecurity risk, while continuing to focus on the board's oversight of the many enterprise-wide risks the company faces.

- **Review Insider Trading Policies.** In connection with the review of disclosure controls and procedures to specifically address cybersecurity incidents (as noted above), companies should also review their insider trading polices and related procedures. One easy fix is to review the list of illustrative "material" events that these policies typically identify and make sure that it includes a cyber example. More substantively, it is important that the individual or individuals responsible for opening and closing trading windows or preclearing trades of the company's securities are in the loop on incidents that have potentially material disclosure implications. While a company itself does not face liability for insider trading by executives and officers, substantial investigation costs, disruptions in work force and the potential loss of important employees can motivate companies to be proactive with their approach to blackouts.

- **Anticipate Staff Comments.** In the Chairman's statement, he noted that he has asked the Division of Corporation Finance to "carefully monitor" cybersecurity disclosures in its filing reviews. Given the disappointment expressed by Commissioners Stein and Jackson (and probably others) that the SEC is not doing more to adopt new disclosure rules, increased staff attention to company disclosures could be one way to respond to that criticism. Companies should consider refreshing their existing disclosures as a way of demonstrating and confirming that they take cybersecurity risks seriously.

Please feel free to contact any member of Ropes & Gray's securities & public companies practice group or privacy & cybersecurity practice group with any questions about this Alert.