Governance & Securities Alert

Weil

From the Public Company Advisory Group of Weil, Gotshal & Manges LLP

February 26, 2018

The SEC Weighs in on Cybersecurity Disclosure:

What's New, What Isn't, and What to Do Now

By Cathy Dixon and P.J. Himbelfarb

The U.S. Securities and Exchange Commission (the "SEC" or "Commission") issued interpretive guidance last week, available here, relating to disclosure of cybersecurity risks and incidents amid increasing cybersecurity threats from cybercriminals, nation-states, competitors and "hacktivists," and a host of significant breaches that have come to light in the last year (including one involving the SEC's EDGAR system). The SEC's guidance is to some extent a repetition of guidance issued in 2011 by the Commission's Division of Corporation Finance ("2011 Staff Guidance"), available here, which enhances its authoritativeness[1], but there are also some new and noteworthy substantive points:

- Focusing on the role of the board of directors, the SEC guidance states that companies should consider the board's oversight of a company's cybersecurity risks and cybersecurity risk management program in drafting proxy statement disclosure of the board's role in risk oversight, to the extent cybersecurity risks are deemed material to a particular company's business.
- The guidance stresses the need for expanded disclosure controls and procedures that function effectively to collect cybersecurity-related information and facilitate its timely analysis by responsible personnel, with a view to determining whether a duty to disclose material non-public information exists.
  - The SEC states that a company's disclosure controls and procedures should cast a wide net to capture information "potentially subject to required disclosure or relevant to an assessment of the need to disclose developments and risks" (emphasis added), and not just information required by specific line items to be disclosed.
  - The guidance further stresses that, while "it may be necessary to cooperate with law enforcement [,]" and recognizes "that the ongoing investigation of a cybersecurity incident may affect the scope of disclosure regarding the incident . . . [,] an ongoing internal or external investigation ***would not*** . . . ***on its own***, provide a basis for avoiding disclosures of a material cybersecurity incident" (emphasis added). As further discussed below, the SEC believes that companies can provide investors with the requisite disclosure without revealing sensitive technological and/or investigative information.

- In an apparent highlighting of incidents at Equifax and Intel, involving executives' sales of securities after discovery but before public disclosure of what, in hindsight, has been viewed as a material cyber breach, the SEC's guidance is directed at prevention of insider trading when a company has undisclosed, potentially material information about cyber risks and incidents, including vulnerabilities and breaches. More specifically, the guidance:
  - reminds companies that information about a company's cybersecurity risks and incidents may constitute material non-public information, and that directors, officers, and other corporate insiders would violate Securities Exchange Act Section 10(b) and Rule 10b-5 thereunder if they were to trade the company's securities while in possession of such material non-public information; and
  - states that companies should "have policies and procedures in place to (1) guard against directors, officers and other corporate insiders taking advantage of the period between the company's discovery of a cybersecurity incident and public disclosure of the incident to trade on material nonpublic information about the incident, and (2) help ensure that the company makes timely disclosure of any related material nonpublic information." Recognizing that many companies have implemented "preventative measures" designed to avoid even the appearance of improper trading, the SEC encourages all companies to consider applying such measures in the context of a cyber event.
- The guidance cautions against selective disclosure of cybersecurity information in violation of Regulation FD and encourages companies to use Form 8-K or Form 6-K to report material cybersecurity matters to the investing public.[2]

The remaining guidance mostly reinforces and expands upon the discussion in the 2011 Staff Guidance:

- Disclosure Obligations Generally; Materiality: Companies should consider the materiality of cybersecurity risks and incidents when preparing periodic reports and registration statements with the SEC. The guidance further states that:
  - the materiality of cybersecurity risks and incidents depends not only upon the nature, extent, and potential magnitude of the risk or incident, but also on the range of harm that such incidents could cause, including harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions;
  - there is no need to include a "roadmap" to future breaches; no disclosure is required of specific, technical information about a company's cybersecurity systems;
  - there is a duty to correct and, although noting a judicial split, possibly a duty to update, when investors are still relying on the prior disclosure; and
  - companies must avoid generic disclosure and instead tailor disclosure to the company's particular cybersecurity risks and incidents.
- Risk Factors: The guidance provides that there are, at a minimum, eight issues to consider in evaluating the need for "significant" cyber-risk disclosure, including, for example, the occurrence of prior cybersecurity incidents.[3] Such past incidents also may need to be disclosed to provide additional context around statements of cybersecurity risk. Companies likewise must consider cybersecurity risk disclosure relating to acquisitions.
- Management's Discussion & Analysis: In the context of known trends and uncertainties, there are a number of items to consider relating to cybersecurity, focusing in particular on costs both of security efforts and preventative measures as well as costs of dealing with incidents (including remediation efforts, addressing harm to reputation, and responding to regulatory investigations). Companies must perform this analysis at the segment level as well.
- Description of Business: The business description should include disclosure of cybersecurity incidents or risks that materially affect a company's products, services, relationships with customers or suppliers, or competitive conditions.

- Legal Proceedings: Cybersecurity litigation should be disclosed if material to the company.
- Financial Statements: Cybersecurity incidents and risks could impact a company's financial statements, including with respect to expenses, loss of revenue, claims, diminished future cash flows, impairment of assets, recognition of liabilities, or increased financing costs.

What to Do Now

- Reexamine the company's cybersecurity-related disclosure in light of the new SEC guidance. While the SEC chose only to issue interpretive guidance at this time, two of the concurring Commissioners expressed a preference for stronger regulatory action by the SEC.[4] Chairman Clayton warned in his public statement, available here, that he has asked the Division of Corporation Finance to continue "to carefully monitor cybersecurity disclosures" and that the Commission "will continue to evaluate developments in this area and consider whether any further guidance or rules are needed."
  - At Practising Law Institute's SEC Speaks conference held Friday, February 23, 2018, a senior Division of Enforcement staff member indicated that the adequacy of company cybersecurity disclosures is on the radar screen of the Division's new Cyber Unit.
- At a minimum, we would expect the SEC staff to "ramp up" the review and comment process in this area and issue more frequently and/or broadly comments similar to those that have been issued in the past, such as urging companies: (1) to tailor the risk factor disclosure and expand the discussion of cybersecurity issues to address, in the MD&A section, the impact of any known trends and uncertainties relating to actual cyber hacks and vulnerabilities; (2) to clarify whether the company has knowledge of the occurrence of attacks in the past and to discuss the costs and consequences of material attacks; (3) to describe the particular aspects of the business and operations that give rise to material cybersecurity risks and the potential costs and other consequences of such risks to those businesses and operations; and (4) with respect to cybersecurity incidents and related litigation, to explain the company's consideration of the GAAP requirement, ASC 450-20-50, to disclose (i.e., in the footnotes to the financial statements) an estimate of the reasonably possible losses or range of loss or to disclose that such an estimate cannot reasonably be made.
- Institutional investors similarly will be monitoring the quality of the company's cybersecurity disclosures, particularly those relating to board cyber-risk oversight responsibilities. The Council of Institutional Investors (CII) included a description of the SEC's interpretive guidance in its latest Weekly Governance Alert, urging members to review its April 2016 report, *Prioritizing Cybersecurity: Five Investor Questions for Portfolio Company Boards*, available here. According to this report, "[i]nvestors should look for a clear delineation of board-level oversight responsibilities in the company's board committee charters and proxy statement risk oversight disclosures."
- Ensure that cyber-breach incidents are elevated to the board level in a timely manner to avoid unpleasant surprises for directors, even if such incidents are still being investigated internally and evaluated for materiality. As the 2016 CII report suggests, large institutional investors will be asking hard questions about the effectiveness of board oversight in the wake of what might prove to be – if only with the 20/20 hindsight of shareholders, customers, vendors and/or regulators – a material cyber-attack. Consider the board's role in overseeing cybersecurity risk in crafting the proxy disclosure required by the SEC rule mandating disclosure of the board's role in risk oversight (Item 407(h) of Regulation S-K).
- Evaluate whether disclosure controls and procedures are effective with respect to cybersecurity. The controls and procedures should flag, for responsible personnel, information regarding what potentially could be a serious cyber breach or risk while such incidents or risks are still being investigated, to facilitate the timely materiality assessment necessary both to enable companies to comply with their disclosure obligations under the federal securities laws, and to consider whether to activate what the SEC termed "preventative measures" in their insider trading policies, such as closing an otherwise open trading window for directors, officers and other corporate insiders.[5]

- Review and revise codes of ethics and insider trading policies and procedures, including but not limited to anti-tipping and Regulation FD compliance provisions, to add actual or suspected cybersecurity incidents as examples of potentially material non-public information subject to prohibitions against selective disclosure and unauthorized trading by designated insiders.

ENDNOTES

[1] Commissioners Robert Jackson and Kara Stein both issued statements, available here and here, expressing disappointment that the guidance was mostly a reiteration of the 2011 Staff Guidance. Commissioner Jackson cited a report by the White House Council of Economic Advisers, available here, which reported its findings that cybersecurity incidents are underreported and that disclosure requirements are too general and do not provide clear instructions on how much information to disclose. Commissioner Stein argued that meaningful disclosure of cybersecurity risks and incidents remains elusive and cited additional guidance that could have been provided, including: disclosure of how technological advances could affect company-specific risks as well as disclosure suggested by the recent Investor Advisory Subcommittee relating to a company's protocols relating to, or efforts to minimize, cybersecurity risks and its capacity, and any measures taken, to respond to cybersecurity incidents; whether a particular cybersecurity incident is likely to occur or recur; or how a company is prioritizing cybersecurity risks, incidents, and defense. Commissioner Stein also suggested that rulemaking is needed as opposed to further guidance.

[2] While foreign private issuers are not subject to Regulation FD, they may be subject to prohibitions against selective disclosure in their home countries in addition to being required to comply with the U.S. antifraud provisions barring insider trading (including tipping, or the unauthorized disclosure of material, non-public information to persons or entities outside the particular company).

[3] The complete list of eight issues identified in the guidance to consider with respect to risk factors are:

- 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.

[4] See note 1.

[5] This will depend heavily upon careful assessment of the relevant facts and circumstances. Companies are experiencing hacks and other cyber-incidents too frequently to close the trading window for every incident, and we do not think that is what the SEC is suggesting. However, we do think the SEC means that this preventative measure (and others the company has in place in its insider trading policies and procedures) should be considered for a significant cyber breach or risk that would be material but where not all the facts are yet known, because the insider trading activities in the public securities markets will be observed (e.g., via the filing of Exchange Act Section 16 reports by officers and directors) and could be challenged later as giving rise to a duty to disclose the particular incident. If a company has reached the conclusion that the trading window must be closed when it would otherwise usually be open, a company also would not allow its executives subject to such closure to enter into Rule 10b5-1 trading plans. While it may still be true that an executive could in good faith represent that she is not aware of any material non-public information at the time she seeks preclearance of such a plan (as yet), such awareness may be imputable to the company. The negative optics and resulting reputational harm to the company of having a sale occur if the cyber-breach or risk is ultimately deemed material and disclosed should be considered in determining whether to allow for the establishment of such a plan.

* * *

Please contact any member of Weil's Public Company Advisory Group or your regular contact at Weil, Gotshal & Manges LLP:

Howard B. Dicker	View Bio	howard.dicker@weil.com	+1 212 310 8858
Catherine T. Dixon	View Bio	cathy.dixon@weil.com	+1 202 682 7147
Lyuba Goltser	View Bio	lyuba.goltser@weil.com	+1 212 310 8048
Adé K. Heyliger	View Bio	ade.heyliger@weil.com	+1 202 682 7095
P.J. Himelfarb	View Bio	pj.himelfarb@weil.com	+1 202 682 7208
Ellen J. Odoner	View Bio	ellen.odoner@weil.com	+1 212 310 8438
Alicia Alterbaum	View Bio	alicia.alterbaum@weil.com	+1 212 310 8207
Kaitlin Descovich	View Bio	kaitlin.descovich@weil.com	+1 212 310 8103
Erika Kaneko	View Bio	erika.kaneko@weil.com	+1 212 310 8434
Reid Powell	View Bio	reid.powell@weil.com	+1 212 310 8831
Niral Shah	View Bio	niral.shah@weil.com	+1 212 310 8316
Aabha Sharma	View Bio	aabha.sharma@weil.com	+1 212 310 8569