PAUL HASTINGS

STAY CURRENT

March 2018

Follow @Paul_Hastings

The SEC Releases New Cybersecurity Disclosure Guidance

By Meagan S. Olsen, Robert P. Silvers, Nick Morgan, Michael L. Spafford, & Peter J. Hegel

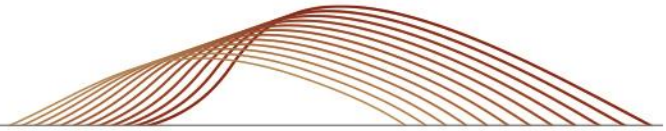
On February 21, 2018, the Securities and Exchange Commission ("SEC") issued an interpretive release (the "Guidance") meant to "assist public companies in preparing disclosures about cybersecurity risks and incidents."[1] Simultaneously affirming and expanding upon the 2011 cybersecurity disclosure guidance issued by the staff of the Division of Corporation Finance,[2] the Guidance aims to clarify cybersecurity disclosure requirements, stress the importance of disclosure controls and procedures related to cybersecurity matters, emphasize the importance of cybersecurity policies and procedures, and address the need for insider trading prohibitions and selective disclosure prohibitions under Regulation FD in relation to cybersecurity incidents.

The Guidance begins by acknowledging the grave threats posed by cybersecurity incidents, including both "unintentional events" and "deliberate attacks."[3] In addition to enumerating a litany of varying cyber threats—including the "use of stolen access credentials, malware, ransomware, phishing, structured query language injection attacks, and distributed denial-of-service attacks"—the SEC crystallizes the "substantial costs and other negative consequences" that can befall a company from vulnerabilities. Importantly, the SEC focuses explicitly on issues that are topics of boardroom discussion, such as increased cybersecurity protection costs, litigation and legal risks; increased insurance premiums; and damage to the company's reputation, competitiveness, stock price, and long-term shareholder value.

With this background, the SEC demands that "public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion."[4] As seen below, these obligations generally constitute a reprise of the 2011 cybersecurity disclosure guidance and the guidelines therein, but offer some new information for companies to act on.

Disclosure Obligations

The Guidance reminds companies of their disclosure obligations under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended, and echoes the staff's 2011 guidance in reminding companies to consider the materiality of cybersecurity issues when preparing disclosures in SEC filings. The Guidance makes it clear that, depending on the particular circumstances, companies may have an obligation to disclose cybersecurity risks and incidents as part of their ongoing disclosure obligations. Some circumstances that would most likely come within the ambit of prescribed disclosure requirements include the following:



- Material risks associated with cybersecurity and cybersecurity incidents, including those "that arise in connection with acquisitions";[5]
- Management's views regarding how the "cost of ongoing cybersecurity efforts (including enhancements to existing efforts), the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents" have affected and will affect the company's financial condition and results of operations;[6]
- Incidents or risks that materially affect a company's "products, services, relationships with customers or suppliers, or competitive conditions";[7]
- Material pending legal proceedings related to cybersecurity issues;
- Cybersecurity incidents and resultant risks that may affect a company's financial statements (including costs related to investigation, remediation and litigation, losses in revenue, resulting legal claims, and diminished future cash flows); and
- The role of the board of directors in overseeing and managing cybersecurity risks when such risks are material to the company's business.

The Guidance reminds companies that, in addition to considering their cybersecurity-related disclosure obligations in the context of specific disclosure requirements, they must also disclose "such further material information, if any, as may be necessary to make the required statements, in light of the circumstances under which they are made, not misleading."[8] While not required to provide detailed information that would serve as a roadmap for hackers, companies are still required to disclose any and all cybersecurity risks that are material to investors.

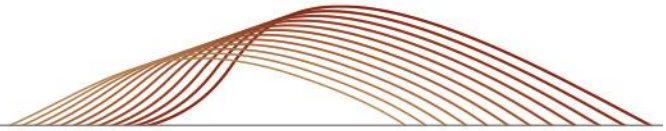
The concept of "materiality" presents a nebulous directive for cybersecurity-related disclosure requirements, but the Guidance directs companies to consider the nature, extent, and potential reputational and financial harm in deciding whether to make a public disclosure in addition to the likelihood of legal or regulatory investigations or actions, and the occurrence of any prior cybersecurity incidents.

Disclosure Controls and Procedures

The Guidance urges companies to ensure that comprehensive cybersecurity policies and procedures are in place and to regularly evaluate their compliance with such policies and procedures as well as the sufficiency of their disclosure controls and procedures to ensure timely disclosure of cybersecurity-related matters. The Guidance states, "Controls and procedures should enable companies to identify cybersecurity risks and incidents, assess and analyze their impact on a company's business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents."[9] Importantly, the Guidance explicitly states that an ongoing internal or external investigation cannot on its own provide a basis to avoid disclosing a material cybersecurity incident, hinting at potential grounds for future enforcement.

Other Areas of Consideration

While the bulk of the Guidance reaffirms directives established in the 2011 cybersecurity disclosure guidance, the SEC acknowledged that it specifically covers new ground with regards to insider trading considerations and selective disclosure requirements.



Insider Trading

The Guidance stresses that "information about a company's cybersecurity risks and incidents may be material nonpublic information"[10] and warns corporate directors, officers, and other corporate insiders that trading the company's securities while in possession of such material nonpublic information would violate antifraud provisions. The SEC suggests that implementing restrictions on trading by insiders in the company's securities may be appropriate during investigations and assessments of cybersecurity incidents.

Selective Disclosure Requirements

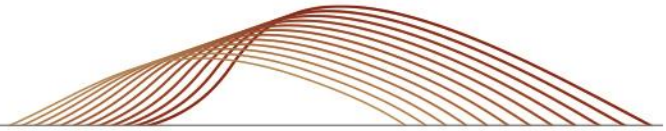
The Guidance clarifies that companies should enact policies and procedures to prevent selective disclosure of material nonpublic information related to cybersecurity risks and incidents: "Under Regulation FD, 'when an issuer, or person acting on its behalf, discloses material nonpublic information to certain enumerated persons it must make public disclosure of that information.'"[11]

Looking Forward

Overall, the Guidance does not create overly burdensome new requirements. Companies with reasonable policies and procedures in place most likely will not need to adopt new policies and procedures based on the Guidance. However, it remains to be seen whether issuance of the Guidance is a prelude to stricter SEC enforcement when it comes to disclosures around cybersecurity risks and incidents. In recent remarks, FBI Director Christopher Wray said, "We don't view it as our responsibility when companies share information with us to turn around and share that information with some of those other agencies," and further remarked that the FBI "[treats] victim companies as victims."[12] We will soon learn whether the SEC under Chairman Clayton likewise views public companies as cyber victims to be protected or as part of the problem to be solved through enforcement.

In the meantime, it is recommended that companies take this opportunity to review their disclosure controls and procedures to ensure that they sufficiently address cybersecurity disclosure, as well as their existing policies and procedures to ensure that insider trading and selective disclosure of material nonpublic information are adequately prohibited. Furthermore, companies—especially boards of directors—should review their cybersecurity risk management policies to ensure that they have a thorough understanding of the cybersecurity risks posed and the policies in place that address such risks.

✧ ✧ ✧



If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Chicago

Peter Hegel
1.312.499.6049
peterhegel@paulhastings.com

Los Angeles

Nick Morgan
1.213.683.6181
nicholasmorgan@paulhastings.com

Meagan S. Olsen
1.213.683.6138
meaganolsen@paulhastings.com

Washington, D.C.

Robert P. Silvers
1.202.551.1216
robertsilvers@paulhastings.com

Michael L. Spafford
1.202.551.1988
michaelspafford@paulhastings.com

---

[1] SEC, *Comm'n Statement & Guidance on Pub. Co. Cybersecurity Disclosures*, Exchange Act Release Nos. 33-10459; 34-82746, 83 Fed. Reg. 8166 (Feb 26, 2018).

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

[3] SEC, *Comm'n Statement*, *supra* note 1. at 8166.

[4] SEC, *Comm'n Statement*, *supra* note 1, at 8167.

[5] SEC, *Comm'n Statement*, *supra* note 1, at 8169 (citing Final Rule: Business Combination Transactions, Exchange Act Release No. 33-6578, 50 Fed. Reg 18990 (May 6, 1985)).

[6] SEC, *Comm'n Statement*, *supra* note 1, at 8170.

[7] *Id.*

[8] SEC, *Comm'n Statement*, *supra* note 1, at 8168.

[9] SEC, *Comm'n Statement*, *supra* note 1, at 8171.

[10] SEC, *Comm'n Statement*, *supra* note 1, at 8171.

[11] SEC, *Comm'n Statement*, *supra* note 1, at 8172 (citing 17 C.F.R. 243.100. Final Rule: Selective Disclosure & Insider Trading, Release No. 34-43154 (Aug. 15, 2000) [65 Fed. Reg. 51716 (Aug. 24, 2000)]).

[12] FBI Chief: *Corporate Hack Victims Can Trust We Won't Share Info*, U.S. News (Mar. 7, 2018, 1:10 PM), https://www.usnews.com/news/technology/articles/2018-03-07/fbi-chief-corporate-hack-victims-can-trust-we-wont-share-info.