Harvard Law School Forum on Corporate Governance

# SEC Increasingly Turns Focus Toward Strength of Cyber Risk Disclosures

*Posted by Vivek Mohan, David Simon, and Richard Rosenfeld, Mayer Brown LLP, on Sunday, July 25, 2021*

**Editor's note:** Vivek Mohan, David Simon, and Richard Rosenfeld are partners at Mayer Brown LLP. This post is based on a Mayer Brown memorandum by Mr. Mohan, Mr. Simon, Mr. Rosenfeld, and Julie L. Sweeney.

On June 11, 2021, the US Securities and Exchange Commission ("SEC" or "Commission") announced that it would focus on cybersecurity disclosures made by public companies as part of its regulatory agenda.[1] Given the SEC's continued interest in cybersecurity issues, high-profile ransomware attacks and executive orders issued by President Biden, it is no surprise that the SEC is focused on taking an increasingly active role in a whole-of-government response to cybersecurity threats. Although it will be some time before a final rule on cybersecurity risk disclosures is issued, a proposal from the SEC is expected in October 2021. In the meantime, public companies should begin preparing for what is likely to be a new SEC rule mandating cybersecurity disclosures.

This Legal Update provides background on the new SEC chairman and the SEC rulemaking process, the SEC's prior guidance on cybersecurity disclosures and steps that public companies can begin taking now to prepare for enhanced SEC oversight of cybersecurity disclosures.

## Background

On April 14, 2021, the Senate confirmed Gary Gensler to be the chairman of the SEC. Shortly thereafter, Chairman Gensler announced an aggressive spring agenda focused on new corporate disclosures for climate change risk, board diversity and workforce diversity. Of particular note is the Commission's clear emphasis on cybersecurity disclosures, or lack thereof, made by public companies.

Although, at this point, it is not certain what will be included in the SEC's proposed rule, in its agenda announcement, the SEC provides a brief description of the rules it intends to propose. The SEC's abstract states that "[t]he Division [of Corporate Finance] is considering recommending that the Commission propose rule amendments to enhance issuer disclosures regarding cybersecurity risk governance."[2]

We will have more insight by October 21, 2021, which is the deadline the SEC has set for issuing its proposed rule. Following this proposal, the SEC will initiate a review and comment period

[1] *See* www.sec.gov/news/press-release/2021-99
[2] *See* www.reginfo.gov/public/do/eAgendaViewRule?pubId=202104&RIN=3235-AM89

during which the public may submit their input. The SEC will consider this input on the proposal as it drafts its final rule.

Though we are months away from a final rule on cybersecurity disclosures, the SEC's last-issued guidance, and subsequent criticism of it, provides helpful context for what may be on the horizon.

## SEC's 2018 Cybersecurity Guidance

In 2018, the SEC adopted long-awaited guidance on cybersecurity disclosure (the "2018 Guidance").[3] This guidance marked the first time that the Commission provided official guidance to public companies about their cybersecurity disclosure obligations. The 2018 Guidance built on the SEC's Division of Corporation Finance 2011 pronouncement—"Disclosure Guidance CF #2—Cybersecurity"[4] (the "2011 Guidance")—which instructed public companies to disclose cyber risks if they "are among the most significant factors that make an investment in the company speculative or risky."[5]

The 2018 Guidance addressed disclosure obligations under existing laws and regulations, emphasized the importance of disclosure controls and procedures and provided instruction on the disclosure of material cybersecurity events and incidents. The guidance also cautioned against insider trading when such material events are not disclosed and against selective disclosure in the context of cybersecurity. Although the 2018 Guidance was adopted unanimously, some of the commissioners at that time made clear that they felt the guidance was not enough.

In a published statement, then-Commissioner Robert Jackson expressed concerns that the 2018 Guidance "essentially reiterates years-old staff-level views on this issue. But economists of all stripes agree that much more needs to be done."[6] He then quoted a 2018 report issued by the White House's Council of Economic Advisers, "The Cost of Malicious Cyber Activity in the U.S. Economy," which described a number of concerns regarding the effectiveness of the 2011 Guidance. For example, the report noted that ambiguity around disclosure requirements and the meaning of "materiality" results in companies generally underreporting cyber incidents.

Likewise, then-Commissioner Kara Stein expressed disappointment that the 2018 Guidance was essentially a rebranding of the 2011 Guidance, which, according to a 2014 study, had "resulted in a series of disclosures that rarely provide differentiated or actionable information for investors."[7] Then-Commissioner Stein also listed some of the ways that the Commission could have done more, including by seeking notice and comment on proposed rules around enhanced board risk management frameworks, timeliness and comprehensiveness of cyber-attack notices to investors and requirements that public companies develop and implement cybersecurity-related policies and procedures beyond just disclosure.

---

[3] *See* www.sec.gov/rules/interp/2018/33-10459.pdf

[4] *See* Div. of Corp. Fin., SEC, CF Disclosure Guidance: Topic No. 2—Cybersecurity (Oct. 13, 2011), www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[5] *Id.*

[6] *See* www.sec.gov/news/public-statement/statement-jackson-2018-02-21

[7] *See* "What Investors Need to Know About Cybersecurity: How to Evaluate Investment Risks," Investor Responsibility Research Center Institute (Jun. 2014), *available at* www.advisorselect.com/transcript/what-investors-need-to-know-about-cybersecurity-how-to-evaluate-invest%ADment-risks/what-investors-need-to-know-about-cybersecurity-how-to-evaluate-investment-risks

At bottom, the 2018 Guidance was just that: guidance. What the SEC is proposing now is a rule that will likely result in cybersecurity disclosures becoming mandatory, along with enhanced scrutiny over past disclosures.

## Looking Ahead

Public companies can look to the 2018 Guidance as an instructive starting point for understanding what the SEC's proposed rule may include. But the SEC is not likely to stop here. It is reasonable to anticipate that the Commission, in consulting with stakeholders, will seek to address and bolster perceived deficiencies in the 2018 Guidance, including by providing clearer instruction on what constitutes "materiality" and "timeliness" of cyber-attack notices.

As noted, a final rule on cybersecurity disclosures is still a ways away. In the meantime, however, here are five steps companies should take to prepare for the SEC's new rule.

1. ***Prepare Criteria for Determining Materiality***. The 2018 Guidance lists certain criteria that public companies should consider when determining whether a cybersecurity incident constitutes a "material" event. These criteria include the nature and magnitude of the incident, along with its financial, reputational or operational ramifications. Public companies should develop and codify an approach to materiality determinations now, as they will be critical in defending future disclosure determinations.
2. ***Review and Enhance Policies and Procedures*.** The 2018 Guidance encourages public companies to develop substantive cybersecurity risk management policies and procedures. Specifically, the guidance provides that these policies should include clear instructions on how to identify and elevate information to key stakeholders and senior leaders so that appropriate disclosures can be made regarding cybersecurity incidents and risks. Companies that incorporated this guidance in 2018 should review whether they are comfortable with their policies and procedures now that this guidance is likely to become mandatory. Companies that have not enhanced their policies must now review the existing policies to expressly consider cybersecurity risks as potentially material and should begin preparing now to review and update their disclosure controls to verify that they are sufficient.
3. ***Enhanced Board Oversight***. The 2018 Guidance states that if "cybersecurity risks are material to a company's business," the board's role in overseeing cybersecurity risks should be disclosed. These disclosures are to address how a board "engages with management on cybersecurity issues" and "discharge[es] its [cybersecurity] risk oversight responsibility." Board members should be encouraged to become more engaged and to take steps to understand the cybersecurity risks throughout their company.
4. ***Enhanced Training***. There is no question by now that companies should be investing in and prioritizing their cybersecurity training and compliance programs. Although companies with strong cybersecurity training and compliance programs cannot guarantee that they will not fall victim to a cyber attack, they can and should take steps to enhance their preparedness for such cyber incidents, including as it relates to any required SEC disclosures.
5. ***Review Past Filings***. Public companies should also consider reviewing their existing periodic filing disclosures to determine whether prior cybersecurity risks and/or incidents that may now be deemed material have been completely and timely disclosed. Companies should review whether there may be material omissions in prior statements.

Despite the fact that the SEC's proposed rule on cybersecurity disclosure will not be public until October, prudent corporate governance, as well as shareholder demand, will drive the shrewd public company to revisit and enhance its cybersecurity disclosure policies and procedures now to be ready for both the inevitable event and the inevitable requirement.