SEC Proposes New Cybersecurity Disclosure Rules For Public Companies

大成 DENTONS

March 22, 2022

SEC Proposes New Cybersecurity Disclosure Rules

The Securities and Exchange Commission ("SEC") recently published proposed rulemaking regarding cybersecurity for (1) investment advisers and funds and (2) public companies. If implemented, these rules will have significant impact regarding cybersecurity governance, risk management by management, oversight by boards of directors, and the maintenance and update of policies, procedures, and compliance programs regarding cybersecurity.

For more regarding the related proposed SEC Rules for Investment Advisers and Funds, please click here.

Public Companies

The SEC proposed amendments to its rules regarding cybersecurity disclosures ("Proposed Amendments") by public companies on March 9, 2022.[1] The Proposed Amendments, if finalized, will require public companies to make new disclosures related to risk management, strategy, governance, and incident reporting. In releasing the Proposed Amendments, the SEC highlighted the investor-demand for insights into the cybersecurity posture of public companies. In fact, the SEC highlighted research that found investors in the United States were more concerned about cybersecurity governance than any other ESG issue.[2]

Prior Guidance

The SEC's Division of Corporation Finance published guidance in 2011 advising companies of materiality considerations for disclosures related to cybersecurity.[3] In 2018, the Commission provided the more substantive and authoritative Statement and Guidance on Public Company Cybersecurity Disclosures ("Interpretive Statement"), which clarified its interpretation of disclosure obligations under the Securities Act of 1933, Securities Exchange Act of 1934, and Regulations S-K and S-X. The Interpretive Statement discussed several existing disclosure obligations which would relate to cybersecurity when material. Still, cybersecurity disclosures may be inconsistent across organizations, and recent SEC inquiries[4] and settlements[5] suggest an increasing regulatory focus on these risks and disclosures. The Proposed Amendments, if finalized, will place specific obligations on companies to be more transparent about cybersecurity risks and incidents.

Proposed Amendments

In a statement about the Proposed Amendments, SEC Chair Gary Gensler noted, “I think companies and investors alike would benefit if [cybersecurity disclosures] were required in a consistent, comparable, and decision-useful manner.”[6] To that end, the Proposed Amendments would impose the following significant requirements[7]:

- **Four-Day Notification Window**. The Proposed Amendments would require organizations to disclose information about a cybersecurity incident via form 8-K within four business days after it determines that it has experienced a material cybersecurity incident. Importantly, the 8-K is not required within four days of the incident itself, only four days after the organization determines the incident is material. Still, the SEC notes in its proposal that many incidents are obviously material as soon as they are discovered. Additionally, the Proposed Amendments require organizations to make the materiality determination “as soon as reasonably practicable” and it expects public companies to make the 8-K disclosures quickly. Organizations may be making public comments on an attack before it has mitigated and remediated the incident, and certainly before an investigation is complete. Unlike many other disclosure laws, the Proposed Amendments make no exceptions for ongoing law enforcement investigations.
- **Quarterly Reporting**. The Proposed Amendments would require organizations to update disclosures relating to previously disclosed cybersecurity incidents via forms 10-Q and 10-K. Additionally, organizations must disclose when immaterial cybersecurity incidents become material in the aggregate on quarterly basis. This quarterly reporting mechanism ensures organizations provide information to investors in a timely manner while recognizing that a victim of a cyberattack will learn significantly more about the incident after it files the form 8-K.
- **Annual Reporting**. The Proposed Amendments would lead to significant changes to what a company must disclose related to cybersecurity in its Form 10-K.
  - *Policies and procedures*. The Proposed Amendments require descriptions of policies and procedures for cybersecurity management. Organizations would need to discuss details including information on its risk assessment programs, risk-management, third-party management, business continuity and disaster recovery plans, and provide information on prior cybersecurity incidents that inform ongoing governance.
  - *Cybersecurity governance*. Organizations would be required to describe its board’s role in overseeing cybersecurity risks including “whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.” The SEC believes that investors will care about how boards of directors are attuned to the cybersecurity risks of their organization.
  - *Managemental information*. Organizations would have to disclose the details of management’s role in assessing and managing cybersecurity risks and implementing policies, procedures, and strategies. This includes providing information on the company’s CISO, including its position in the organizational chart and expertise.
  - *Board cyber expertise*. When applicable, companies would have to disclose individual board members with specialized expertise related to cybersecurity. Helpfully, the Proposed Amendments would not impose any duty on a board member with cybersecurity expertise beyond the duties of any other board member and such designation does not alleviate any duties other board members have to the company.
  - *Special rules for foreign private issuers*. Foreign private issuers would have modified Form 20-F and Form 6-K disclosure requirements substantially similar to those of domestic companies as set forth above.

What to Do Today

The Proposed Amendments highlight increasing regulatory expectations regarding disclosures regarding cybersecurity risks. Though the new rules are not yet in effect, complying with the Proposed Amendments or

subsequent rulemaking may require a paradigm shift at many organizations.

1. *Prepare for broader and more specific disclosures regarding cyber incidents.*
   Companies should closely review cybersecurity, data and technology risk factors to ensure that cybersecurity risks relating to internal corporate systems, products and services, and supply chains are appropriately and accurately disclosed in sufficient detail. Policies and procedures should also be updated to help ensure that senior leadership and boards have access to key, relevant, and timely information regarding cybersecurity risks, *prior* to making disclosure decisions. Reporting requirements in such policies and procedures should take into account these periodic reporting schedules and also require significant incidents to be escalated to leadership more swiftly based on risk, to aid in a continuous evaluation of whether such significant incidents have crossed the materiality threshold and require disclosure under the Proposed Rule.

2. *Review and revise your Cybersecurity Program.*
   If the Proposed Amendments are finalized, public companies will have to provide significant details of their internal policies and procedures on managing cybersecurity risk, not just disclosure of such risks. Companies should develop or update policies and procedures that are based on appropriate best practices and trusted standards and that are reasonable in light of industry risks, so they can be fully operational prior to making public disclosures about them. Companies also should consider updating their ESG charters to address cybersecurity risk.

3. *Implement continuous improvement models in your systems development lifecycle.*
   Though not expressly stated, continuous improvement is an undercurrent of the Proposed Amendments. Annually, the SEC will require disclosures of prior incidents that inform existing policy. Quarterly, the SEC will ask for any changes in the policies and procedures borne out of previously disclosed cybersecurity incidents and will require details on how the incidents may have informed such changes. Continuous improvement methods will help an organization learn from past incidents and explain how those lessons inform a more resilient organization. Tabletop exercises can help identify opportunities to further enhance incident response planning and cybersecurity risk management, to help before an incident occurs.

4. *Commenting on the Proposed Amendments; Monitor developments.*
   The SEC is accepting comments on the Proposed Amendments until May 8, 2022 (60 days following publication of the proposing release on the SEC's website), or 30 days following publication of the proposing release in the Federal Register, whichever period is longer. Interested parties may wish to contact counsel to help prepare comments or submit them directly to the Office of Management and Budget Desk Officer for the U.S. Securities and Exchange Commission and the Secretary of the SEC. Dentons will continue to monitor these developments.

---

[1] Proposed Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule ("Proposed Amendments"), available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

[2] Proposed Amendments at fn 21.

[3] CF Disclosure Guidance: Topic No. 2 https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[4] For example, the inquiry directed to numerous companies beginning in June 2021, in In the Matter of Certain Cybersecurity-Related Events, https://www.sec.gov/enforce/certain-cybersecurity-related-events-faqs.

[5] For example, regarding the SEC's August 2021 settlement with Pearson, https://www.sec.gov/news/press-release/2021-154.

[6] Gary Gensler, SEC Chair, Statement on Proposal for Mandatory Cybersecurity Disclosures, March 9, 2022, https://www.sec.gov/news/statement/gensler-cybersecurity-20220309.

[7] These requirements would modify 17 CFR Parts 229, 232, 239, 240, and 249.

Your Key Contacts

Allison J. Bender
Partner, Washington, DC
D +1 202 496 7362
allison.bender@dentons.com

Ira L. Kotel
Partner, New York
D +1 212 398 5787
ira.kotel@dentons.com

Jeffrey A. Baumel
Partner, New York
D +1 212 768 5374
jeffrey.baumel@dentons.com

Donald A. Hammett, JR. PC
Partner, Dallas
D +1 214 259 0917
M +1 214 415 7201
donald.hammett@dentons.com

Victor H. Boyajian
Global Chair, Venture Technology and Emerging Growth Companies, New York
D +1 212 768 5349
M +1 650 815 5146
victor.boyajian@dentons.com

Kyle W. Miller
Of Counsel, Louisville
D +1 502 587 3517
kyle.miller@dentons.com