wiley

ALERT

SEC Proposes Cybersecurity Rules for Publicly Traded Companies

March 10, 2022

What: Publicly traded companies may soon be subject to additional cybersecurity reporting requirements. On March 9, 2022, the Securities and Exchange Commission (SEC) proposed rules and amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies after finding that current disclosure practices are inconsistent. The proposals recognize that cybersecurity is an emerging risk for public companies and that both companies and investors need to evaluate public companies' cybersecurity practices and incident reporting. The SEC's proposed rules and amendments are part of the increasing number of reporting requirements the government is issuing to mandate disclosure of cybersecurity incidents.

What does it mean for industry: The SEC is joining the growing number of federal agencies playing a role in cybersecurity. The SEC seeks to require public companies to: (1) disclose information about a material cybersecurity incident within four business days after the company determines that it has experienced a material cybersecurity incident; (2) provide updated disclosure relating to previously disclosed cybersecurity incidents; and, (3) disclose when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate.

In addition to the cybersecurity incident reporting requirements, the proposal would also require public companies to regularly report on the roles of management and the board of directors on cybersecurity policy. Specifically, public companies would be required to: (1) describe its policies and procedures, if any, for the identification and management of risks from cybersecurity threats; (2) disclose the

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
jfbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Privacy, Cyber & Data Governance

Securities Enforcement and Litigation

board's oversight of cybersecurity risk and management's role and expertise in assessing and managing cybersecurity risk and implementing the registrant's cybersecurity policies, procedures, and strategies; and, (3) disclose in annual reports and certain proxy filings if any member of the registrant's board of directors has expertise in cybersecurity.

Public comments will be due 60 days following publication of the proposal's release on the SEC's website or 30 days following publication of the proposal's release in the Federal Register, whichever period is longer.

What impact will the SEC's proposed rules have?

The proposed amendments are designed to better inform investors about public companies' cybersecurity risk management, strategy, and governance and to provide timely notification of material cybersecurity incidents. The SEC believes that consistent, comparable, and decision-useful disclosures would allow investors to evaluate public companies' exposure to cybersecurity risks and incidents as well as their ability to manage and mitigate those risks and incidents.

"Over the years, our disclosure regime has evolved to reflect evolving risks and investor needs," said SEC Chair Gary Gensler. "Today, cybersecurity is an emerging risk with which public issuers increasingly must contend. Investors want to know more about how issuers are managing those growing risks. A lot of issuers already provide cybersecurity disclosure to investors. I think companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner. I am pleased to support this proposal because, if adopted, it would strengthen investors' ability to evaluate public companies' cybersecurity practices and incident reporting."

The SEC's proposals kick off a public comment period on the following:

- **Incident Disclosure Amendments**:
  - The SEC would require registrants to disclose information about a material cybersecurity incident within four business days after the public company determines that it has experienced a material cybersecurity incident by amending Form 8-K;
  - The SEC would require public companies to provide updated disclosure relating to previously disclosed cybersecurity incidents and to require disclosure, to the extent known to management, when a series of previously undisclosed individually immaterial cybersecurity incidents have become material in the aggregate by adding new Item 106(d) of Regulation S-K and Item 16J(d) of Form 20-F; and,
  - The SEC seeks to add "cybersecurity incidents" as a reporting topic to Form 6-K.
- **Risk Management, Strategy, and Governance Disclosures**
  - The SEC would require that public companies describe their policies and procedures, if any, for identifying and managing risks from cybersecurity threats, including whether the companies consider cybersecurity as part of their business strategy, financial planning, and capital allocation; and,

- The SEC wants to require that public companies disclose the board's oversight of cybersecurity risk and management's role and expertise in assessing and managing cybersecurity risk and implementing cybersecurity policies, procedures, and strategies by adding Item 106 to Regulation S-K and Item 16J to Form 20-F.
- The SEC proposes to require disclosure of board members' cybersecurity expertise by amending Item 4076 of Regulation S0K and Form 20-F.

Key Takeaways

The federal government is increasingly requiring the private sector to enhance cybersecurity through disclosure obligations, incident reporting, and attempting to establish *de facto* standards of care. Implicit in the government's now more frequent issuances is the notion that the private sector is unwilling or unable to implement sound cybersecurity risk management processes without federal guidance, rules, and or regulations.

Companies should expect to see SEC enforcement investigations and civil litigation regarding the timing and manner of exactly when a public company determined it experienced a "material cybersecurity incident" given the four-day reporting requirement. We anticipate this will lead to an increase in insider trading investigations related to trading around the ultimate disclosure of the event. We also anticipate possible investigations and fraud allegations regarding management's level of expertise and the status of a companies' cyber policies.

Public companies have a limited period of time to comment on the SEC's proposed cybersecurity rules and amendments. Public comments will be due 60 days following publication of the proposal's release on the SEC's website or 30 days following publication of the proposal's release in the Federal Register, whichever period is longer.