Centri

SHARE

March 2022

SEC Proposes New Requirements for Cybersecurity Risk Management, Governance, and Incident Disclosure

On March 9, 2022, the U.S. Securities and Exchange Commission (SEC) proposed new cybersecurity rules regarding disclosure requirements for public reporting companies. The proposed rules are part of an increased initiative for companies to prioritize a commitment to their cybersecurity risk management program and to provide investors clearer visibility into key cybersecurity practices and incident reporting.

Key takeaways from the complete 129-page proposed rules that public companies should be aware of and prepared for include:

Reporting of material cybersecurity incidents and periodic reporting to provide updates about previously reported cybersecurity incidents

- Filers would be required to amend Form 8-K to report a material cybersecurity incident within four business days after registrants have determined that they have experienced such an incident. (Note that the proposed rule states that the required reporting period is within four business days *after the company has determined that a material incident has occurred*, not within four business days of first discovery). Proposed Item 1.05 provides that "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident."
- Requirement for updates on previously reported material cybersecurity incidents through registrant's 10-Ks and 10-Qs for the period in which the update occurred.

Disclosure of cybersecurity risk management strategies

- Proposed requirements for disclosure about the companies' cybersecurity policies and procedures for identifying and managing cybersecurity risks and threats. Proposed Item 106(b) would require disclosures of whether:
  - The registrant has a cybersecurity risk assessment program, and if so, provide a description of such program;
  - The registrant engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program;
  - The registrant has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider, including, but not limited to, those providers that have access to the registrant's customer and employee data;
  - The registrant undertakes activities to prevent, detect, and minimize the effects of cybersecurity

incidents, and if so, provide a description of the types of activities undertaken;
    - The registrant has business continuity, contingency, and recovery plans in the event of a cybersecurity incident;
    - Previous cybersecurity incidents informed changes in the registrant's governance, policies and procedures, or technologies;
    - Cybersecurity-related risks and previous cybersecurity-related incidents have affected or are reasonably likely to affect the registrant's strategy, business model, results of operations, or financial condition, and if so, how; and
    - Cybersecurity risks are considered as part of the registrant's business strategy, financial planning, and capital allocation, and if so, how.

Disclosure of cybersecurity governance

- Proposed requirements for disclosure about a registrant's cybersecurity governance, including the board's involvement and oversight over cybersecurity risk.
- Disclosure of a description of management's role in assessing and managing cybersecurity risks, the relevant expertise of such management, and its role in implementing the registrant's cybersecurity policies, procedures, and strategies.

The public comment period will remain open for 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.

What proactive steps should companies be considering?

- Confirm that adequate policies and procedures over cybersecurity have been developed and implemented, and that the company is performing a cyber risk assessment on a periodic basis.
- Assess the Board of Directors' current role in cybersecurity oversight, including requirements to determine if any board members are considered "cyber experts."
- Develop or update your Incident Response Plan to include initial and periodic reporting requirements (including incident disclosures on Form 6-K for foreign private issuers).
- Create a methodology for determining if a cybersecurity event constitutes a material incident.
- Update SEC disclosure checklists to comply with the proposed new cybersecurity reporting rules.
- Develop and implement a vendor risk management program.
- Ensure that a qualified member of management has been assigned with responsibility for overseeing cybersecurity.

Please contact Centri for more information or to explore how our expertise in SEC Compliance & Reporting and Cybersecurity Risk Management aligns with the specific needs of your company.