SEC's Cybersecurity Amendments Will Introduce Detailed Reporting Obligations

On March 9, 2022, the Security and Exchange Commission (SEC) proposed new rules to improve upon and standardize cybersecurity-related disclosure obligations for public companies. The SEC is expected to finalize the rules in April 2023, which means registrants should begin working now to bring their reporting practices in line with the new requirements. Below is a high-level overview of certain upcoming changes introduced by the SEC's disclosure amendments.

Cyber Incident Reporting

- The SEC will amend Form 8-K to require disclosure of information regarding material cybersecurity incidents within four days of a registrant's discovery of an incident. In determining "materiality," the SEC instructs registrants to carefully and objectively assess each incident to determine, among other things, whether "there is a substantial likelihood that a reasonable shareholder would consider it important." While not exhaustive, the SEC provides a list of examples that may constitute a material incident:
  - An incident that compromises the confidentiality, integrity or availability of information;
  - An incident that causes the degradation, interruption, loss of control, damage to or loss of operational technology systems;
  - An unauthorized party, or party exceeding the scope of their authorization, accesses, alters or steals sensitive information that may result in loss or liability for the registrant;
  - An incident where a threat actor offers to sell or publicly disclose sensitive data, and
  - An incident where a threat actor demands a ransom payment.
- Regulation S-L and Form 20-F will be revised to require registrants to provide updates on previously disclosed cybersecurity incidents. Additionally, registrants must now report multiple immaterial cybersecurity incidents when they become material in the aggregate.
- Form 6-K will be amended to add "cybersecurity incidents" as a reporting topic.

Risk Management, Strategy, and Governance Reporting

- Regulation S-L and Form 20-F will be amended to require a description of a registrant's policies and procedures for mitigating and managing cybersecurity threats. The description should account for the registrant's business strategy, financial plan and capital allocation as they pertain to risk mitigation.
- The SEC will also require disclosures regarding the board of director's oversight of cybersecurity risk mitigation and management of the registrant's policies, procedures and strategies.

- Finally, board members will have to report their level of cybersecurity expertise on annual reports and certain proxy filings. This report must include the names of any board members with cybersecurity experience and any details required to describe the nature of the expertise.

Bond attorneys regularly assist and advise clients on an array of data privacy and cybersecurity matters, including regulatory reporting. If you have any questions regarding the SEC's upcoming cybersecurity disclosure requirements, please contact Jessica Copeland, CIPP/US, Mario Ayoub or any attorney in Bond's cybersecurity and data privacy practice.

BOND SCHOENECK & KING ATTORNEYS