CADWALADER

Cabinet **News and Views**

Informed analysis for the financial services industry

## SEC Amendments on Cybersecurity Disclosure

By **Peter Bariso**
Associate | Corporate

At an open meeting last week, the Securities and Exchange Commission (the "SEC") proposed amendments "to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies." Recognizing the growing risk of cybersecurity in today's digitally connected world, SEC chair Gary Gensler spoke on the benefits to investors of consistent and comparable disclosure on (i) material cybersecurity incidents affecting public companies and (ii) public companies' cybersecurity risk management policies, strategy and governance.

If adopted as proposed, public companies would be required to disclose cybersecurity incidents, update previously disclosed incidents and describe the company's cybersecurity policies and strategy. The SEC proposal defines "cybersecurity incident" broadly to include any "unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein."

If adopted as proposed, the amendment would require, among other items:

- **Current Disclosure:** Upon the occurrence of a material cybersecurity incident, a company would be required to file a current report on Form 8-K within four business days, and disclose:
    - when the incident occurred or was discovered;
    - the nature and scope of the incident;
    - whether any data was stolen, altered, accessed or used for an unauthorized purpose;
    - the effect of the incident on the company's operations; and

    - whether the company has remediated or is currently remediating the incident.

- **Periodic Disclosure:** As part of the SEC's periodic reporting regime, a company would be required to disclose on its quarterly reports on Form 10-Q and annual reports on Form 10-K:

    - updates to previously disclosed material cybersecurity incidents or instances where any previously undisclosed immaterial incidents have become material;

    - the company's policies and procedures for the identification and management of risks from cybersecurity threats;

    - identification of cybersecurity experts on the board, if any, and information on board oversight of cybersecurity policies and risks; and

    - management's role and expertise in assessing and managing cybersecurity risk and implementing the company's cybersecurity policies, procedures, and strategies.

If adopted as proposed, foreign private issuers would also be subject to the new cybersecurity disclosure as part of the Form 6-K and Form 20-F filing requirements.

The current proposed amendments are focused on mandating previous SEC disclosure guidance of cybersecurity policies and risks and do not prescribe cybersecurity practices that companies must follow or outline any minimum standard for public companies. Additionally, if adopted as currently proposed, failure to timely file a required Form 8-K upon the occurrence of a material cybersecurity incident would not cause a company to lose Form S-3 eligibility to register securities. Before any final rule is promulgated, a 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.

The full text of the rule is available here.

---