SEC DISCLOSURE REQUIREMENTS

On July 26, 2023, the SEC established a major turning point in corporate cybersecurity response by introducing detailed rules on cyber risk management, strategy, governance, and incident disclosure. These regulations compel SEC-registered companies to disclose their board's oversight of cybersecurity risks, extending responsibility beyond chief information and security officers.

Key aspects of these rules include:

1. **Incident Reporting:** Companies must report significant cybersecurity events within four business days after recognition, focusing on the incident's material impacts rather than specific details.
2. **Third Party Incidents:** Disclosure is required for cybersecurity incidents on third-party systems, with no exemption for information on these systems.
3. **Previously Disclosed Incident Reporting:** Firms must update information on past cybersecurity incidents, particularly their impact on business operations and finances.
4. **Series of Undisclosed Incidents:** Disclosure is necessary when multiple minor cybersecurity incidents collectively become significant, including their discovery time, status, and a brief overview.
5. **Policies and Procedures:** Businesses need to outline their cybersecurity risk and threat management approaches, covering a range of risks and detailing any risk assessment programs.
6. **Governance:** Companies must reveal information about board and management oversight of cybersecurity risk, including management's role, expertise, and implementation of cybersecurity strategies.
7. **Management's Role:** Descriptions of management’s responsibilities in assessing, managing, and implementing cybersecurity policies and strategies are required.

SEC DISCLOSURE REQUIREMENTS

Item	Summary Description of the Disclosure Requirements
Regulation S-K Item 106(b)– Risk management and strategy	• Detail methods for evaluating, identifying, and handling significant cybersecurity risks. • Indicate if cybersecurity risks have significantly impacted, or are likely to impact, business plans. • Describe effects on operational outcomes and financial status due to cybersecurity threats.
Regulation S-K Item 106(c) – Governance	Registrants are required to: • Outline how the board oversees risks associated with cybersecurity threats. • Detail the role of management in evaluating and handling significant cybersecurity risks.
Form 8-K Item 1.05 – Material Cybersecurity Incidents	Registrants are obligated to: • Report any material cybersecurity incident they experience. • Describe key details of the incident, including its nature, extent, timing, and the actual or likely impact. • They must submit an Item 1.05 Form 8-K within four business days after recognizing the incident as material. However, if the U.S. Attorney General concludes that immediate disclosure would significantly endanger national security or public safety, the filing can be postponed as specified. • Furthermore, if there is new or previously unavailable information related to a reported incident, registrants must update the initial Item 1.05 Form 8-K filing with this information.
Form 20-F	Foreign Private Issuers (FPIs) are required to: • Explain how their board supervises risks related to cybersecurity threats. • Detail the involvement of management in identifying and addressing significant cybersecurity risks.
Form 6-K	Foreign Private Issuers (FPIs) need to: • Outline the methods their board uses to oversee cybersecurity risk. • Describe how their management team assesses and manages major cybersecurity threats.