U.S. Risk, LLC

NEWS ALERT

Expected Spring 2023: New SEC cybersecurity reporting requirements for publicly traded companies. Cybersecurity related business activities, decision-making processes and the Board's role in oversight would be subject to heightened transparency and reporting requirements.

CYBERSECURITY: REPORTING BREACHES TO THE SEC

Public companies need to prepare for the reporting of cyber breaches to the SEC as soon as new requirements are enacted. The proposed new rules include:

- Requirements to notify the SEC of any "material" cybersecurity event within four business days.
- Public company Board of Directors must oversee and participate in the evaluation, assessment and implementation of cybersecurity policies and procedures.
- Mandatory disclosures about management's role in addressing cybersecurity risk.

› What Makes a Cyber Incident "Material"

Who will decide what is "material" is still a bit blurry. While the SEC has not yet provided specifics, it has stated that a) determining materiality is both a quantitative and qualitative exercise, and b) that materiality is around what a reasonable investor thinks is material, not necessarily what a CISO or the CFO thinks is reasonable.

Quantitative factors can include the amount of data compromised, the number of downed systems, and the how critical are these systems. Qualitative factors include whether the company's reputation or brand has been harmed, any ransom paid, any law enforcement, supplier, or customer notifications.

› Take Steps Now

- Review cybersecurity and risk management documentation. Examine how incidents have been handled in the past to identify and practice what will need to be done differently moving forward.
- Review the company's incident response plans. Examine how the company would respond to breaches, ransomware, and other cybersecurity incidents.
- Determine what "material" means to the organization.
- Educate the company's Board of Directors to ensure they are equipped to oversee the organization's policies and processes.

Under new rules expected to be finalized soon, publicly traded companies that determine a cyber incident has become "material"—meaning it could have a significant impact on the business—must disclose details to the SEC and investors within four business days.