CAC Specialty™

CLIENT ALERT

SEC FINALIZES NEW RULES ON CYBER SECURITY RISK MANAGEMENT AND DISCLOSURE

JULY 28, 2023

On July 26, 2023, the Securities and Exchange Commission (SEC) announced that it had finalized new rules on cyber security risk management, strategy, governance, and incident disclosure by public companies.

The new rules require public companies to disclose any cyber security incident that is determined to be material, as well as describe the aspects of the incident and its impact on the company. In the rule, the SEC defined information as being material "if there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would have significantly altered the 'total mix' of information made available."

The timeline for disclosure is four business days after the company designates the event as being material. However this disclosure may be delayed if the US Attorney General determines that the disclosure would pose a risk to national security or public safety. Most public companies will be required to start providing these 8-K and 6-K disclosures by December 18, 2023. Smaller companies will have an additional 180 days before they need to provide the 8-K disclosure going forward.

Additionally, public companies will also be required to disclose on an annual basis material information regarding cyber security processes for assessing, identifying, and managing risks from cyber security threats, as well as the effect of risks from cyber security threats and previous incidents.

Also required is information on board of directors' oversight as it relates to risks from cyber security threats, and management's role and expertise in assessing and managing those risks. These disclosures in Form 10-K or 20-F will be due for annual reports for fiscal years ending on or after December 15, 2023.

While these new disclosure regulations are intended to increase transparency for investors, there is concern that the disclosure of material impacts of breaches can be instructive to the threat actors perpetrating the breaches themselves.

CAC Specialty recommends that you reach out to your broker to discuss the impact of these new disclosure requirements, especially with regards to the following:

- Potential for increased personal liability for directors and officers
- Potential for increased exposure to shareholder derivative and class action litigation
- Limits considerations for D&O and Cyber insurance coverages
- Data and analytics tools available relative to cyber risk quantification

For more information, please reach out to your CAC Specialty contact.

We're here to help. Let's connect.

Atlanta | Boston | Chattanooga | Chicago | Cincinnati | Dallas | Denver | Eugene
Houston | Knoxville | New York | Portland | Scottsdale | San Francisco | Seattle | Summit