We **blogged** last week as soon as the SEC adopted its new cyber disclosure rules about seven quick things you needed to know. And now we have put out a much **more in-depth Client Update** about these important new rules. Here's an excerpt from that:

- **Materiality Determinations Must Be Made Without Unreasonable Delay**

The nature and timing of materiality determinations are important areas of focus. The materiality threshold for cybersecurity incidents will be consistent with the standard analysis in securities law: information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" to investment decision-making. In the cybersecurity context, a materiality assessment may take into account factors such as impact on operations and financial condition; reputational harm; effect on competitiveness or relationships with

customers and vendors; potential litigation or regulatory action; and loss of data, assets, or intellectual property.

Critically, the new rule requires registrants to make materiality determinations "without unreasonable delay" after discovery of the incident. The SEC acknowledges that "in the majority of cases, the registrant will likely be unable to determine materiality the same day the incident is discovered" and requires registrants to develop information relevant to materiality without unreasonable delay. The final rules provide a few examples of what would or would not be considered unreasonable delay. For example, the SEC states in the final rules that "a company being unable to determine the full extent of an incident because of the nature of the incident or the company's systems, or otherwise the need for continued investigation regarding the incident, should not delay the company from determining materiality."

Additionally, the SEC states that if the materiality determination is to be made by a board committee, the committee may not intentionally delay meeting to make a materiality determination past the normal time it takes to convene a meeting of its members. A company also may not revise existing incident response policies or procedures "in order to support a delayed materiality determination for or delayed disclosure of an ongoing cybersecurity event."

And then here are some "Key Take-Aways" from the Update:

- **Practical Tips: What Should Companies Do Now To Prepare**

Although implementation of the final rules is a few months off yet, companies should begin considering the impending new disclosure requirements. Here are some ways to prepare:

1. Review and update company disclosure controls and procedures to ensure information regarding possible material cyber incidents are timely reported to those in charge of making disclosure decisions.
2. Evaluate the board's oversight structure and consider whether oversight of cybersecurity risks should be assigned to a committee if it is not already. Also, keep in mind that any such changes should be disclosed in upcoming proxy statement disclosure.
3. Review and update as necessary the company's cybersecurity risk management processes, including at both the board and management levels.
4. Consider developing a materiality matrix to assist in determining whether a cybersecurity incident is material.
5. Prepare a draft of the new Form 10-K disclosure well in advance of the Form 10-K filing deadline.

Explore more in

Corporate Law
Blog series

Public Chatter

Public Chatter provides practical guidance—and the latest developments—to those grappling with public company securities law and corporate governance issues, through content developed from an in-house perspective.

View the blog