Blogs
September 25, 2023

In addition to the "**Deep Dive Into the SEC's Materiality Trigger" Client Update** that I blogged about last week, we now have a new Client Update by David Aaron entitled "**Updating Corporate and Cybersecurity Practices To Satisfy the SEC's Final Cybersecurity Disclosure Rules: Assessing Materiality of Cybersecurity Incidents**." Check it out! [Don't forget this Thursday's webcast: "**The SEC's New Cyber Disclosure Rules – What To Do Now**."]

Here's an excerpt: "Based on the SEC's advice, an affected company and its IR team should incorporate the following guidance when assessing materiality:

- Take a **holistic** view of materiality.
    - Do not rely exclusively on quantitative thresholds.
    - Does the type of data affected create particular risk?
    - Does the type of system affected create particular risk?
    - Does a cybersecurity event have a direct impact on operations or the value of the company?
    - Does a cybersecurity event create downstream risk to the confidentiality, integrity, or availability of customer data or systems?
    - Does that event create longer-term risk for the value of the company?
        - Impact on competitiveness based on theft of intellectual property (IP) or customer lists.
        - Loss of customer confidence in privacy of information.
        - Loss of customer confidence in security and/or continuity of operations.
        - Impact on reputation.
        - Impact on vendor relationships.
    - Does the event expose a security flaw or other information that contradicts representations the company has previously made?
        - Does the fact or nature of the compromise expose the company to potential liability for prior statements, actions, or inaction regarding security?
    - Does the event raise the likelihood of litigation, regulatory action, or investigations?
- A company can have sufficient information to determine that an incident is material **before an investigation is complete**. Possessing sufficient information makes the company responsible for making that determination promptly and starts the reporting clock.
    - A company should not wait to report until a full IR or investigation concludes if the company has sufficient information to make a materiality determination.
    - If "crown jewels" or key operational systems have been compromised, a company probably knows enough to make a materiality determination. This knowledge may well start the reporting clock even if a full investigation is not yet complete.
    - If an unauthorized actor has had access to or exfiltrated a large amount of important data, a company similarly probably has sufficient information to determine that an incident is material, and the reporting clock may start even if the full investigation is not yet complete.
    - The scenarios in the SEC release did not distinguish between encrypted and unencrypted data. Whether or not the affected data is encrypted, and whether or not an unauthorized actor possesses or obtains the key, will affect the materiality analysis but may not be dispositive.

- Although the SEC "streamlined" the substantive reporting requirements and imposed a short deadline, ensure that the report is **not misleading, including by omission**.
    - Legal and technical cybersecurity personnel in particular should probe IR teams' conclusions. For example, is a statement that a certain repository was not affected based on affirmative evidence, a lack of evidence, or inability to conduct analysis before the reporting deadline? If structured data fields were encrypted or otherwise protected, what about free text fields?
    - Identifying "known unknowns" in the initial report and filing an amended report once those gaps are filled is acceptable and contemplated by the new rule, as long as the review and determinations are not unreasonably delayed.
    - It is essential to file corrections—either of inaccurate statements or material omissions—promptly.

- When assessing whether an incident is material, following "**normal internal practices and disclosure controls and procedures** will suffice to demonstrate good faith compliance."
    - A company should not change assessment or reporting criteria during an incident response for a purpose that appears to be delaying the required report.
    - If a board committee or other group must be convened to make the determination, a company should not defer or delay the meeting beyond the time it would usually take to convene the group.
    - For third-party incidents, there is no need to gather information outside of "regular channels of communication" with the relevant third-party service provider.

- Resolve doubt as to whether information is material **in favor of disclosure**.
- If a company is aware that reportable information has not been determined or is not available by the reporting deadline, it should **identify known gaps** in the report it files with the SEC and file an amended report when it has additional information.
- Do not assume that sharing threat information with private sector or government entities implies that a company has determined an incident to be material. The SEC clearly stated that alerting other parties of a threat does not in and of itself trigger a reporting obligation if the impact on the company is not material."

### 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