SQUIRE PATTON BOGGS

Who Determines Materiality of Cybersecurity Incidents in Light of Recent SEC Rule Requiring Disclosure of Cybersecurity Incidents?

⁝ 26/06/2024

New SEC Rule Imposes Four Day Deadline to Disclose Material Cybersecurity Incidents

In December 2023, the U.S. Securities and Exchange Commission's ("SEC") new rule requiring disclosure of material cybersecurity incidents became effective. SPB previously analyzed how the new rule applies to incidents affecting third-party vendors and what companies can do to manage reporting risks created by third-party cybersecurity incidents. In the first half of 2024, more than a dozen companies reported cybersecurity incidents pursuant to the new rule using the new Item 1.05 in the updated Form 8-K. The new Item 1.05 requires an issuer to disclose specific information about a cybersecurity incident within four business days of its determination that the incident is material. This new rule makes the materiality determination pivotal in a company's response to a cybersecurity incident and raises an important question about who should be involved in making the pivotal determination.

Who Makes Materiality Determination?

Notably, new Item 1.05 does not set forth whether management or directors should make the materiality determination. Similarly, other recent SEC and U.S. Department of Justice ("DOJ") guidance has not dictated to issuers who must make the determination. However, issuers should be aware of a general recent trend toward encouraging increased director involvement in cybersecurity matters.

Additionally, since a cybersecurity incident may present an enterprise-level risk, and the board of directors is ultimately responsible for the enterprise, the directors should be involved and informed in the event of any potentially major cybersecurity incident so that they can properly exercise their oversight responsibilities. Some companies may prefer to have the board of directors make the formal materiality determination in the event of a major cybersecurity breach. Others may prefer to have management make the determination, particularly where consultation with the full board of directors may be too cumbersome in a fast-moving situation. The absence of specific SEC or DOJ guidance as to who makes the determination seemingly acknowledges that there is no one size-fits-all solution. Whatever the company's approach, it is critical that it is set forth in company policies and/or procedures so that the company has clear guidelines before a cybersecurity incident arises.

If management is charged with making the materiality determination, the board of directors, or at least some subset of directors (i.e. the board chair, audit committee chair, full audit committee, or some

combination thereof) should be briefed and given an opportunity to provide advice and counsel either prior to the determination or shortly thereafter. Notice and consultation with the board of directors allows the directors to exercise necessary oversight of the enterprise and can also ensure that the organization is properly aligned as it responds to the cybersecurity incident.

Conclusion

As companies consider the recent SEC rule update and how they can best respond to cybersecurity incidents, they should choose an approach that best fits their unique structure, personnel, policies, and needs. Companies should also review their cybersecurity response policies and procedures and ensure that they reflect the company's chosen approach. Companies should update any outdated policies promptly to reflect new procedures. While no single approach can work best for all organizations, boards or directors should be involved and consulted on cybersecurity incidents and responses.