BARNES & THORNBURG LLP

Securities and Capital Markets Blog
PRACTICAL SECURITIES LAW

SEC Declines To Require Identification Of Cybersecurity Expertise On Board

August 28, 2023

By Taylor Wirth

As we previously blogged about, the Securities and Exchange Commission (SEC) adopted final rules requiring the disclosure of material cybersecurity incidents and cybersecurity risk management, strategy, and governance by public companies.

Final rules rolled back disclosure requirement regarding director cybersecurity expertise

The final rules significantly streamlined many of the proposed prescriptive disclosure items, including the controversial proposal that would have required disclosure of whether any member of the registrant's board of directors has cybersecurity expertise. Proposed Item 407(j) of Regulation S-K did not define what constitutes such expertise, although the proposing release included a non-exhaustive list of criteria to consider, including prior work experience, relevant degrees or certifications, any knowledge, skills or other background in cybersecurity.

The proposal garnered significant pushback and was generally viewed as being overly prescriptive. For example, some commenters argued that cybersecurity risk was not "intrinsically different from other risks that directors assess with or without specific technical expertise." In addition, there were concerns that the disclosure item "would pressure companies to retain cybersecurity experts on their board" but that there were not enough cybersecurity expert board nominees. Also, some commenters flagged that the requirement could result in decreased diversity on corporate boards.

The SEC was persuaded to drop the proposed rule, acknowledging that such disclosure may not be material for all companies, that "effective cybersecurity processes are designed and administered largely at the management level, and that directors with broad-based skills in risk management and strategy often effectively oversee management's efforts without specific subject matter expertise, as they do with other sophisticated technical matters."

Survey of large companies

Where does this leave public companies with respect to their disclosure

RELATED PRACTICE AREAS

Corporate
Securities and Capital Markets

RELATED TOPICS

SEC
Cybersecurity

practices? We surveyed the 25 largest companies in the Fortune 500 and found that practice varied with respect to describing the board's cybersecurity expertise, although we noticed a few trends in recently filed proxy statements.

- Skills Matrix: In their director skills matrix, a slight majority of these companies either expressly included cybersecurity or cybersecurity was referred to under a complementary qualification, such as Technology, eCommerce, Risk Management, Privacy, Security or Information Technology. The remaining companies did not include or refer to cybersecurity as a qualification in their matrix, although virtually all companies included risk management as a key skill, which presumably would encompass cybersecurity or technology security matters.

- Director Biography: Only one-third of the top 25 companies specifically highlighted cybersecurity expertise in a director's biography in the proxy statement. Of these, only a handful described with specificity how the board member or nominee gained their cybersecurity skill, e.g., achieved certification from the National Association of Corporate Directors (NACD) or another academic certification, or by virtue of past employment, including military service.

Practical takeaways

Whether or not a director's cybersecurity expertise should be highlighted in SEC filings is a nuanced decision specific to each company.

- Counsel should consider whether the disclosure that would have been required under Item 407(j) would be helpful for investors even though the SEC did not adopt the rule. Practitioners are reminded that existing Item 401(e) of Regulation S-K elicits disclosure regarding "the specific experience, qualifications, attributes or skills that led to the conclusion that the person should serve as a director … in light of the registrant's business and structure." Additionally, the disclosures required under new Regulation S-K Items 106(b) [cybersecurity risk management and strategy] and 106(c) [cybersecurity-related governance] may provide sufficient information for investors without the need for director-specific expertise. Based on these items and the company's industry, operations and particular risk profile, Items 106(b), 106(c) and 401(e) may nonetheless result in disclosure of a director's cybersecurity expertise.

- Given investor and SEC scrutiny on cybersecurity matters, consider whether to update your board skills matrix to address cybersecurity (either as a standalone category or refining an existing category to reference cyber matters).

- In connection with the proposed rules, some companies updated their D&O questionnaires to elicit information from directors or nominees in order to determine whether that person had cybersecurity experience (even if the questions were for internal informational purposes only). Companies may consider adding or retaining such questions if cybersecurity expertise is a qualification that is material to the company's risk management and strategy or governance.