The SEC’s New Cybersecurity Disclosure Rules

Description

Lawrence A. Cunningham

All public company directors should be aware of the new requirements on cybersecurity disclosure the SEC adopted last week. To its credit, the SEC exercised considerable restraint in ensuring that its new rules are better seen as fostering good practices rather than dictating corporate behavior.

Unfortunately, cyberattacks have become routine, with public companies targeted daily. Most public companies have a senior manager with a staff responsible for cybersecurity — reflected in the latest C-suite acronym, the CISO, or chief information security officer. CISOs regularly report incidents to fellow executives, and summaries are usually presented to the board in quarterly meeting decks.

When the CISO determines that a cyber incident may be material — whether in quantitative financial terms or harm to reputation or relationships — the team elevates the problem internally, including to the board. When judged to be material, a company publicly discloses information about such effects.

These materiality determinations have become standardized since 2018, when the SEC began encouraging public companies to make such assessments. Management’s assessment and internal reporting invariably detail the threat and related vulnerabilities, but companies have no duty to disclose such matters, lest disclosure provide a blueprint more helpful to hackers than investors.

The new SEC rules impose related disclosure requirements. Public companies will be required to disclose the material impacts of material cyberattacks within four days after a company’s determination...
that an incident was material. Directors might ask CISOs and general counsel how they are preparing for this requirement, such as how to determine materiality and what information to consider supplying about incidents.

In annual reports, public companies will need to add a section on cybersecurity processes, which will describe management’s expertise and approach to cybersecurity and risk mitigation as well as any board oversight in this area and how management notifies the board of related risks. Directors will recognize this as the standard approach to corporate governance: Management is responsible for managing while directors are duty-bound to oversight.

Diligent directors ought to educate themselves on cybersecurity, including through company-sponsored board training programs. Public company boards should receive periodic updates from senior managers on cybersecurity defenses, threats and incidents and discuss how the company’s cybersecurity relates to its overall risk management process.

The SEC took great care in its new rules to stress its function as the provider of mandatory disclosure frameworks without getting into the regulation of corporate governance. In its official release adopting the rules, the commission explained: “[W]e confirm that the purpose of the rules is . . . to inform investors, not to influence whether and how companies manage their cybersecurity risk.”

In that spirit, these new rules are far more focused and balanced than the initial sweeping proposals the SEC made in March 2022. As the SEC emphasized in its official release, the final rules “help avoid levels of detail that may go beyond information that is material to investors and address commenters’ concerns that those details could increase a company’s vulnerability to cyberattack [and] to foreclose any perception that the rule prescribes cybersecurity policy.”

For example, the new disclosure requirements focus not on the details of an incident (its status, remediation, data compromised or system vulnerabilities), which would provide blueprints for hackers, but on impact on the company, which would be of interest to investors. Similarly, as finalized, the rules eliminate a proposal that would have required companies to aggregate multiple immaterial incidents if they would be material when aggregated — a proposal fraught with unnecessary complexity and cost.

The final rules also lean toward a streamlined approach to disclosing board oversight and governance processes, responding to what critics of the proposal said was a prescriptive and invasive approach. For example, no disclosure is required concerning the frequency of board discussions of cybersecurity or the relative expertise of any board member or the board in the field of cybersecurity. Concerning disclosure of expertise, the SEC credited numerous concerns of critics, including:

1. “Cybersecurity risk is not intrinsically different from other risks that directors assess with or without specific technical expertise.”

2. Such a “disclosure requirement would [unduly] pressure companies to retain cybersecurity experts on their board.”

3. “Identified expert directors would face elevated risks, such as being targeted by nation-states for surveillance or hackers attempting to embarrass them.”
4. The rule was “overly prescriptive.”

The SEC concluded, “We are persuaded 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.”

While the final rules are more streamlined than proposed, some critics are unconvinced that they strike the right balance. Critics include two of the five SEC commissioners, who voted against the proposal. They worry that the rules remain too prescriptive, create risks of premature disclosure of incidents and could provide roadmaps to hackers, and that the resulting disclosure could hurt rather than help investors. Cybersecurity remains a vital business issue for public companies, and their boards should continue as before to be diligent in their oversight of this area. Managers should likewise continue to scrutinize and continuously upgrade their current cybersecurity safeguards to stay steps ahead of the fiendishly creative bad actors posing ubiquitous threats.

Date Created
August 3, 2023

Author
lawcunningham