SEC's final cybersecurity rules: A board lens

The final rules impose significant disclosure requirements that will require more robust oversight by the board

Summary of final rules

Material cybersecurity incidents to be reported on Form 8-K

Public companies will be required to report information regarding a material "cybersecurity incident" within four business days after the company determines that the incident was material—not from the time of discovery of the incident. And companies must make materiality determinations "without unreasonable delay" after discovery of the incident. Information to be disclosed includes a description of the material aspects of the nature, scope, and timing of the incident, as well as the material impact (or reasonably likely material impact) on the company, including its financial condition and results of operations. Satisfying the deadline for materiality determinations could challenge management teams—particularly in situations where facts continue to unfold and the company is still responding to the cyber incident. Companies will need to create new or revised internal and disclosure controls and ensure coordination among the cyber team, securities lawyers, lawyers assisting the cyber team, and the management disclosure team to make timely materiality determinations.

Companies had expressed concerns about making disclosures if law enforcement requested a delay or national security were implicated, but the final rules only include a narrow exception. If the US Attorney General determines that immediate disclosure poses a substantial risk to national security or public safety and notifies the SEC in writing, disclosure may be delayed for a maximum of 60 days (absent extraordinary circumstances). As a practical matter, such an expedited determination from the US Attorney General will be difficult to obtain. Companies also will not be required to disclose information that has been classified by a department or agency of the Federal government for the protection of the interest of national defense or foreign policy as a result of existing SEC Rule 0-6 under the Exchange Act.

Updated incident disclosures on an amended Form 8-K are required for any new information about a previously disclosed material incident that was unavailable or undetermined at the time of the initial Form 8-K filing.

Cybersecurity risk management, strategy, and governance disclosures

Companies must describe in their Form 10-K their processes for assessing, identifying, and managing material risks from cybersecurity threats, as well as the material effects or reasonably likely material effects of risks from cybersecurity threats and previous cybersecurity incidents. While companies will not be required to disclose board-level cybersecurity expertise, they will be required to describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats.

Effective dates

Companies will be required to make Form 8-K cyber incident disclosures beginning the later of 90 days after the date of publication in the Federal Register or December 18, 2023. Smaller reporting companies will have an additional 180 days before they must begin providing the Form 8-K disclosure. All public companies will be required to make Form 10-K annual disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023.

Form S-3 Eligibility; Safe Harbor

Untimely reporting of material cyber incidents on Form 8-K filings will not jeopardize a company's ability to use a short-form registration statement on Form S-3. And the new rules provide a limited safe harbor from securities law liability since management will have to make a rapid materiality determination.

Monitoring management's preparations to comply

The final rules greatly expand companies' cybersecurity disclosure obligations. While many companies began preparations some time ago, preparations to comply with the final rules will be a significant undertaking for management, and board oversight will be essential. We highlight the following areas for board attention:

Cybersecurity governance disclosures

The final rules require that, in its Form 10-K, a company "[d]escribe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks." In preparation for this disclosure, boards should reassess how the board—through its committee structure—assigns and coordinates oversight responsibility for the company's cybersecurity risk. Boards are taking various approaches to oversight of cybersecurity risk. For many, oversight is housed with the audit committee . Even if cybersecurity oversight is housed with the full board or a different committee, such as a technology committee, the audit committee will still need to oversee the effectiveness of internal and disclosure controls and procedures relating to cybersecurity. When multiple committees are involved, information sharing, communication, and coordination among committees and with the full board is essential. The board should help ensure the necessary processes are in place to accomplish this.

The governance disclosure must also describe management's role in assessing and managing the company's material risks from cybersecurity threats. The final rules state that in providing the disclosure, the company should address, as applicable:

The preparation of these governance disclosures will take time and care, and likely require a reassessment of the board's and management's current cybersecurity governance processes, as well as existing governance disclosures.

whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise

the processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and

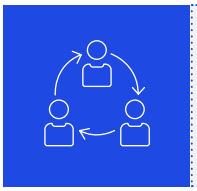
whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

Boards should be working with management teams now as management prepares for the upcoming Form 10-K disclosures.

Cybersecurity risk management and strategy disclosures

The final rules require that a company describe in Form 10-K its processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. The rules state that, in providing such disclosure, a company should address, as applicable, the following non-exclusive list of disclosure items:

whether and how any such processes have been integrated into the company's overall risk management system or processes



whether the company engages assessors, consultants, auditors, or other third parties in connection with any such processes; and

whether the company has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.

The rules also require that the company describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company, including its business strategy, results of operations, or financial condition.

The preparation of these risk management and strategy disclosures will require a reassessment, and perhaps modification, of the company's existing risk management processes and related disclosures. Again, boards should be working with management now as management prepares for the upcoming Form 10-K disclosures.

Management's cyber incident response plan

Management's cyber incident response policies and procedures, including disclosure controls and procedures, must be reviewed and updated to provide for the timely consideration of materiality—at the same time that management is engaged in remediation and investigation efforts. This would include a clear delineation of responsibilities of management's cybersecurity and risk management teams, management's disclosure committee, and the legal department, as well as escalation procedures for determining materiality and the preparation and review of disclosures. Escalation protocols should also include when the board is notified and how internal and external communications are handled. Management and the board should conduct tabletop exercises to test management's response plans and procedures, including protocols for documenting incidents, evaluating for materiality, and drafting Form 8-K disclosures—and refine response plans and procedures to reflect what is learned from those exercises. Incident response plans should also be updated to take into account the changing cyber risk landscape.

Consideration of "materiality."

The final rules require companies to make a materiality determination "without unreasonable delay after discovery of the incident." While the definition of materiality has not changed, applying that standard in the context of a cybersecurity incident is not straightforward. In its final release, the SEC said that companies should consider qualitative factors in assessing the material impact of an incident, and indicated that harm to a company's reputation, customer or vendor relationships, or competitiveness, and the possibility of litigation or regulatory investigations or actions, may be examples of material impacts. Audit committees and boards should confirm that management has in place policies and procedures for making the materiality determination, including the identification of significant cyber incidents that should be escalated and discussed with management's disclosure committee and legal team for final materiality determination, and documenting its materiality determinations.

The role and composition of management's disclosure committee

Given the expanded cybersecurity disclosure obligations, companies may need to reconsider who serves on management's disclosure committee and the role and responsibilities of the committee in developing and maintaining cybersecurity-related disclosure controls and internal controls and procedures. What resources and processes does the committee require to make a timely determination of materiality in the event of a cyber incident?

Expansion of management's subcertification process to support CEO and CFO quarterly certifications regarding design and operational effectiveness of disclosure controls (including internal controls) and procedures

Management's disclosure committee supports quarterly CEO and CFO certifications of the effectiveness and design of the company's internal controls and disclosure controls and procedures required by Section 302 of the Sarbanes-Oxley Act. The disclosure committee typically maintains a subcertification process involving cascading subcertifications from employees regarding the company's internal controls to support the CEO and CFO certifications. Given the expanded scope and detail of the company's required cybersecurity disclosures, the subcertification process should be expanded, as necessary, to obtain new cybersecurity-related subcertifications.

Reference link:

https://boardleadership.kpmg.us/relevant-topics/articles/2023/sec-final-cybersecurity-rules-a-board-lens.html

Contact us

John H. Rodi
Leader, KPMG Board Leadership Center, KPMG US
T: 312-203-3732
E: jrodi@kpmg.com

Claudia H. Allen
Senior Advisor, KPMG Board Leadership Center, KPMG US
T: 312-659-7407
E: claudiaallen@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia