KIRKLAND & ELLIS

Kirkland Alert

SEC Issues Final Rules on Cybersecurity Disclosure for Public Companies

28 July 2023

On July 26, 2023, the SEC adopted final rules that require public companies to report material cybersecurity incidents within four days. The new rules also require annual disclosure of a company's processes to assess, identify and manage material cybersecurity risks, management's role in assessing and managing material cybersecurity risks, and the board of directors' oversight of cybersecurity risks. Foreign private issuers will be subject to similar reporting requirements in Forms 6-K and 20-F, as described below.

Public companies should work with counsel and technical consultants to assess their cybersecurity incident response programs and be prepared to comply with more robust and timely SEC disclosure requirements while not compromising the effectiveness of response or remediation plans.

The compliance date for the Form 8-K and Form 6-K cybersecurity reporting requirement will be the later of 90 days (or 270 days for smaller reporting companies) after publication in the Federal Register or December 18, 2023 (with such disclosures required to be XBRL tagged by the later of 465 days after publication in the Federal Register or December 18, 2024). The periodic disclosures will be required in annual reports for fiscal years ending on or after December 15, 2023 (and the periodic disclosures will be required to be XBRL tagged in annual reports for fiscal years ending on or after December 18, 2024).

Notable Changes from the Proposed Rules

The SEC made a number of changes to the proposed rules in response to the comment letters it received. The SEC:

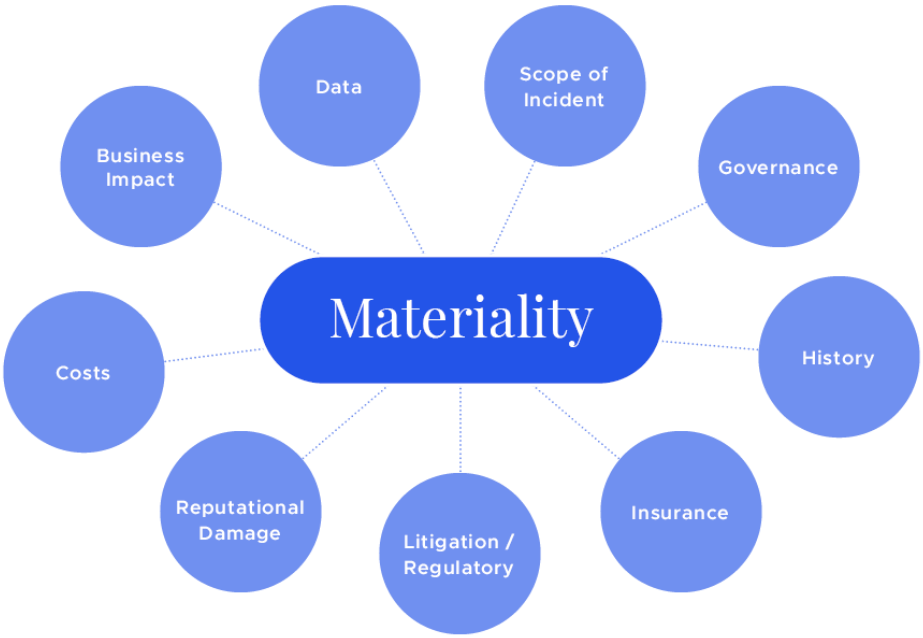
- narrowed the scope of incident disclosure;
- added a limited delay for disclosures that would pose a substantial risk to national security or public safety;
- required certain updated incident disclosure on an amended Form 8-K/6-K (instead of on Form 10-Q/10-K/20-F);
- omitted aggregation of immaterial incidents for the materiality analysis;
- streamlined the risk management, strategy and governance disclosure requirements; and
- did not adopt the proposed requirement to disclose board cybersecurity expertise.

Overview of SEC's New Cybersecurity Disclosure Requirements

Disclosures of Material Cybersecurity Incidents

The final rules require a company to file a Form 8-K within four business days of a determination that a cybersecurity incident it has experienced is material. Specifically, the new Form 8-K 1.05 line item requires disclosure of the (1) nature, scope and timing of the incident and (2) its impact or reasonably likely impact on the company.

The final rules do not specify how to determine the materiality of a cybersecurity incident. Instead, materiality is to be evaluated based on the total mix of information, as is the case with other materiality determinations under federal securities laws. Depending on the circumstances, some of the factors companies may want to take into account when making a materiality determination may include:



Under the final rules, companies must amend a previously filed Item 1.05 Form 8-K to disclose any information called for in Item 1.05 that was not determined or was unavailable at the time of the initial Form 8-K filing.

A company may delay an Item 1.05 Form 8-K only if the U.S. Attorney General notifies the SEC in writing that immediate disclosure would pose a substantial risk to national security or public safety.

This new requirement to file a current report within four days of determining that a company has experienced a material cybersecurity incident does not reflect current practice and may be difficult and onerous for companies to comply with when faced with a cybersecurity incident that is already a strain on resources. Companies should discuss in advance of the rule's effectiveness how best to approach such an incident and evaluate whether a current report is required in order to ensure that ad hoc decisions are not made absent a deliberative process and with inconsistent results.

Safe Harbors

The final rules include two provisions that potentially mitigate liability concerns associated with the proposed new requirements. First, untimely disclosure of material cybersecurity incidents on Form 8-K would not result in a loss of Form S-3 eligibility. Similarly, untimely disclosures of material cybersecurity incidents are eligible for a limited safe harbor from liability under Section 10(b) or Rule 10b-5.

Disclosures Regarding Cybersecurity Risk Management and Strategy

The final rules require companies to disclose information regarding their cybersecurity risk management strategies. Specifically, the new rules add a new Item 106(b) to Regulation S-K to require a description of (1) a company's processes, if any, for the assessment, identification and management of material risks from cybersecurity threats, and (2) whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations or financial condition.

Disclosure Regarding Cybersecurity Governance

The final rules require disclosure regarding a company's cybersecurity governance at both the board and management levels. New Item 106(c) of Regulation S-K requires disclosure of (1) the board's oversight of risks from cybersecurity threats and (2) management's role in assessing and managing material risks from cybersecurity threats. While the SEC did not adopt the proposed requirement to disclose board expertise, the final rule will require disclosure of the relevant expertise of those responsible for the company's cybersecurity management.

Applicability to Foreign Private Issuers

Foreign private issuers will be required to furnish on Form 6-K information on material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange or to security holders. They will also be required in Form 20-F to (1) describe the board's oversight of risks from cybersecurity threats and (2) describe management's role in assessing and managing material risks from cybersecurity threats.

Key Cybersecurity Takeaways

How to Navigate Effective Cybersecurity Incident Response and the New Disclosure Requirements

The requirement in the final rules to disclose the existence and key details surrounding a material cybersecurity incident within four business days of determining that an incident is material underscores the importance of ensuring effective disclosure controls and procedures are in place to escalate potentially material events to senior legal and business leaders to ensure accurate and timely reporting. Companies will need to determine quickly whether an incident is material such that a Form 8-K is required, and if disclosure is required, how to ensure that it meets SEC requirements while not compromising the effectiveness of its response or remediation plans. Helpfully, the SEC's final rules specifically indicate that companies will not be expected to disclose specific, technical information about their incident response or their cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede their response or remediation efforts.

In addition, close coordination with internal and outside counsel after discovery of a cybersecurity incident will be critical as ongoing internal or external investigations, such as investigations by law enforcement, would not, under the final rules, excuse a delay in disclosure (unlike state data breach notification laws). The only delay permitted under the final rules will be if the U.S. Attorney General determines immediate disclosure would pose a substantial risk to national security or public safety.

Does the Board Need a Cyber Committee and Members with Cyber Expertise?

The final rules will require disclosure of the board's oversight of risks from cybersecurity threats. While the SEC abandoned the proposed requirement to disclose the board's cybersecurity expertise, some companies have questioned whether the SEC expects that a robust cybersecurity program needs to be overseen by a dedicated cyber committee with cyber experts. We do not believe that all companies must recruit cybersecurity experts or establish cybersecurity committees. Like with other areas of risk management, we expect that boards will take a thoughtful and company-specific approach to determining an effective and appropriate structure for oversight of cybersecurity risk, including increasing board-level education on cybersecurity, deep-dive discussions with management, and external programs or presentations from law enforcement and other third-party experts on the threat environment, attack trends and common vulnerabilities.

Potential Management Actions to Address Cybersecurity Threats

Although the SEC does not prescribe best practices for cyber governance, we anticipate companies will develop strategies, policies and procedures to manage and mitigate cybersecurity risk. Companies may conduct regular cybersecurity risk assessments to assess readiness for a cyber incident, the response plan and a recovery plan. Companies may also practice cyber incident response readiness through regular tabletop exercises. Companies often ensure adequate resource allocation through annual budgeting and human capital planning, but each company will need to develop its own practices that create effective and appropriate cybersecurity protocols for its organization. Companies will also need to build out appropriate disclosure controls to comply with new SEC disclosure rules.

Potential Board Actions to Address Cybersecurity Threats

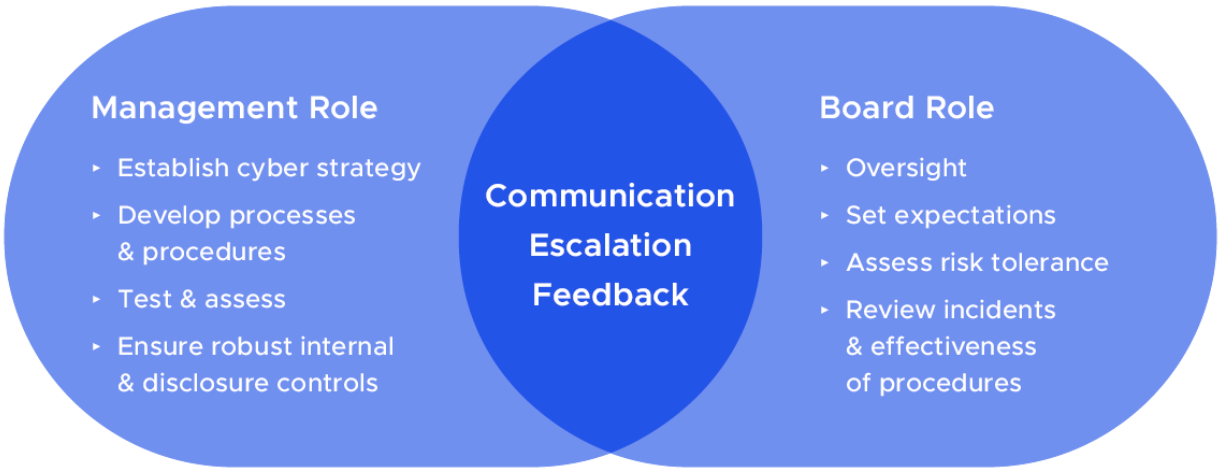
A company's board of directors may insist on good information and effective dashboards and ensure cyber risk is embedded in strategic decisions and the company's culture — including important aspects relating to changing operations, entering new markets, developing new products and services, making acquisitions, and messaging from the top. The board may meet with the company's CISO and CIO and ask about:

- Near misses, not just big breaches;
- How they develop and retain talent;
- Vendors security issues as well as vendor diligence for suppliers of cloud, mobile, hosting and SaaS providers; and
- Controls surrounding business functions and what steps will be taken in the event of an incident.

Boards focused on these issues may meet with business unit leaders on a rotating basis and ask how they approach cybersecurity risk, as well as discuss identified risks with management, including risk prioritization, appetite and mitigation strategies, and cyber insurance.

Good governance practices vary based on individual circumstances, but the following diagram sets forth some of the common roles often played by management and the

board when it comes to cybersecurity management and oversight:



How Should a Company Integrate Cybersecurity into its Disclosure Controls?

Companies should evaluate their existing disclosure controls and procedures in light of SEC's final cyber rules to:

- Identify relevant stakeholders and assign responsibility;
- Review existing frameworks for escalating and analyzing cybersecurity-related data;
- Prepare an incident response plan that incorporates materiality determinations at an early stage;
- Design, implement and test heightened disclosure controls; and
- Train employees to recognize and escalate issues.

Kirkland & Ellis attorneys from across various practice groups work together to advise public companies and other clients on cyber threat preparedness and cyber incident response. Please contact us to discuss developing or evaluating your cyber strategy and implementing management and board actions in response to these new rules.

Authors

Sophia Hudson, P.C.

Partner / New York

Erin Nealy Cox, P.C.

Partner / Dallas / Washington, D.C.

Sunil Shenoi

Partner / Chicago

Christine Strumpen-Darrie

Partner / New York

Christina M. Thomas

Partner / New York / Washington, D.C.

Related Services

Practices

- Transactional
- Capital Markets

Suggested Reading

16 November 2023 Sponsored Event Financing Wind Offshore Conference 2023

22 September 2023 Speaking Engagement American Bar Association's Environmental Transactions Masterclass

21 September 2023 - 22 September 2023 Speaking Engagement 2023 Proxy Disclosure & 20th Annual Executive Compensation Conferences