KIRKLAND & ELLIS

Kirkland Alert

SEC Proposes New Cybersecurity Disclosure Regime for Public Companies

14 March 2022

- The SEC recently proposed rules that would for the first time specifically mandate current and periodic reporting of material cybersecurity incidents and would also require periodic disclosure of a company's cybersecurity risk management policies, strategy and governance and board cybersecurity expertise.
- Public companies should consider working 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.

On March 9, 2022, the SEC proposed rules that would create a new cybersecurity disclosure regime applicable to public companies. Substantially expanding on prior interpretative guidance, the new rules, if adopted, would for the first time specifically mandate current and periodic reporting of material cybersecurity incidents, and would also require periodic disclosure of a company's policies and procedures to identify and manage cybersecurity risks, management's role and expertise in implementing cybersecurity policies, procedures, and strategies, and the board's oversight role and cybersecurity expertise, if any.

While the proposed rules are not yet effective and a comment period is now open, given heightened policy and investor interest in cybersecurity related matters in recent years, the proposed requirements are likely to be adopted in a form that is generally consistent with the proposal. This note provides a brief overview of the proposed rules and key takeaways for public companies to consider in anticipation of final rules being implemented.

Overview of SEC's Proposed Cybersecurity Disclosure Requirements

Disclosures of Material Cybersecurity Incidents

The proposed rules would 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 line item would require disclosure of (1) when the incident was discovered and whether it is ongoing; (2) the nature and scope of the incident; (3) whether any data was stolen, altered, accessed or used for any other unauthorized purpose; (4) the effect of the incident on the company's operations; and (5) whether the company has remediated or is currently remediating the incident.

The proposed 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. The proposed rules do, however, provide examples of incidents that could be material, such as accidental exposure or theft of sensitive business information, intellectual property or personally identifiable information, threats to sell or publicly disclose sensitive data, and ransomware demands.

Under the proposed rules, any material changes or updates to cybersecurity incidents that were previously disclosed must be disclosed in subsequent Form 10-Q and Form 10-K reports. In addition, a series of individually immaterial cybersecurity incidents that later become material in the aggregate would need to be disclosed in subsequent Form 10-Q and Form 10-K reports.

Disclosures Regarding Cybersecurity Risk Management and Strategy

The proposed rules would also require companies to disclose more information regarding their cybersecurity risk management strategies. Specifically, the new rules would amend Regulation S-K to require a description of a company's policies and procedures, if any, for identifying and managing risks from cybersecurity threats, including (1) operational risk; (2) intellectual property theft; (3) fraud; (4) extortion; (5) harm to employees or customers; (6) violation of privacy laws and other litigation and legal risk; and (7) reputational risk.

In addition, the proposed rules specify a series of items that must be disclosed, including a description of the company's cybersecurity risk assessment program, whether the company engages third parties to assess its cybersecurity program, and whether the company's financial condition is reasonably likely to be affected by cybersecurity risks and incidents.

Disclosure Regarding Cybersecurity Governance

Additionally, the proposed rules would require disclosure regarding a company's cybersecurity governance at both the board and management levels. With respect to board oversight, the proposed rules would require disclosure of (1) whether the entire board, specific board members or a board committee is responsible for the oversight of cybersecurity risks; (2) the processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic; and (3) whether and how the board or a board committee considers cybersecurity risks as part of its business strategy, risk management and financial oversight.

With respect to management's role, the proposed rules would require specific disclosures, including (1) specifying management roles responsible for cybersecurity, including whether the company has a chief information security officer (CISO) or similar role; (2) processes by which responsible persons are informed about and monitor the prevention, mitigation, detection and remediation of cybersecurity incidents; and (3) whether and how frequently such persons report to the board or applicable board committee on cybersecurity risk.

Disclosures Regarding Board Expertise

The proposed rules would also require disclosure about the cybersecurity expertise of members of the board, if any. The proposed rules do not define "cybersecurity expertise" but provide several factors to consider, such as prior work experience or certifications in cybersecurity. Such disclosures would be required in both the company's proxy statement and Form 10-K.

Safe Harbors

The proposed rules include three 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. Finally, directors who are disclosed as having cybersecurity expertise would not qualify as experts under federal securities laws – in the proposing release, the SEC indicates that the purpose of this safe harbor is to clarify that the proposed rules would not impose any greater liability or obligations on directors carrying the cybersecurity expertise label (and conversely, that a board's identification of a cybersecurity expert does not reduce the obligations or liabilities of any other director).

Applicability to Foreign Private Issuers

Under the proposed rules, the foregoing requirements would also generally apply to foreign private issuers (FPIs).

Key Takeaways in Anticipation of Final Rules

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

The proposed requirement 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 (1) implementing a tailored incident response plan in advance of an incident and (2) engaging with counsel immediately after an incident is discovered. In particular, companies should work with counsel to determine 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 proposing release specifically indicates that companies would 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 counsel will be critical as ongoing internal or external investigations, such as investigations by law enforcement, would not, under the proposed rules, excuse a delay in disclosure (unlike state data breach notification laws). At the same time, the proposal solicits comments on whether public disclosure could be delayed if requested by the Attorney General due to national security concerns. We expect this issue could yield significant comments and could lead to potential revision of the notification requirement.

Do Companies Need to Hire Cybersecurity Consultants?

The proposed rules do not identify cybersecurity best practices for public companies, nor do they prescribe cybersecurity practices that companies must follow. However, the proposal identifies a series of items that must be disclosed about companies' cybersecurity risk management strategies (if applicable) and these items could signal the SEC's expectations regarding cybersecurity programs, while compulsory

disclosure could impact market practice and investor expectations. For example, the SEC's proposal requires companies to describe whether they use third parties in connection with their cybersecurity risk assessment programs. If the rules are adopted as proposed, companies should not read them to require the retention of cybersecurity consultants. Instead, we recommend that companies consult with counsel and members of their technical teams about the appropriateness of their cybersecurity programs, allowing the resulting disclosure to reflect the board and management's thoughtful and company-specific approach to cybersecurity risk management.

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

Similarly, while the proposed rules would require disclosure if any board members have cybersecurity expertise and whether cybersecurity risk oversight is overseen by the full board, a board committee or specific members, they should not be read as a pronouncement that all companies must recruit cybersecurity experts or establish cybersecurity committees. Like with other areas of risk management, boards should take a thoughtful and company-specific approach to determining an effective and appropriate structure for its oversight of cybersecurity risk.

Authors

Sophia Hudson, P.C.

Partner / New York

Edward J. Lee, P.C.

Partner / New York

Shaun J. Mathew, P.C.

Partner / New York

Sunil Shenoi

Partner / Chicago

Related Services

Practices

- Government, Regulatory & Internal Investigations
- Cybersecurity & Data Privacy
- Mergers & Acquisitions

Suggested Reading

- 11 March 2022 Press Release Kirkland Counsels Admiral on Completion of Delaware Basin Assets Sale to Petro-Hunt
- 10 March 2022 Press Release Kirkland Advises 17Capital on Strategic Partnership with Oaktree
- 10 March 2022 Press Release Kirkland Counseled TPG Rise Climate on its Investment in Monarch Bioenergy RNG Joint Venture