GUNDERSON DETTMER

SEC Proposes Mandatory Cybersecurity Disclosure Framework for Public Companies

Insights
April 6, 2022

Comprehensive Suite of Proposals Would Require Enhanced and Standardized Disclosures Regarding Cybersecurity Risk Management, Strategy, Governance and Incident Reporting, Including Form 8-K Disclosure of Material Cybersecurity Incidents Within Four Business Days

---

Key Takeaways

- The Securities and Exchange Commission ("SEC" or "Commission") recently proposed rules that would, for the first time, expressly mandate cybersecurity disclosures by public companies, including current and periodic reporting about their material cybersecurity incidents, cybersecurity risk management, strategy and governance practices, and board cybersecurity expertise.
- The proposed disclosure mandates are intended to elicit more timely, informative, consistent and comparable information that investors can use to better differentiate companies' preparedness and ability to manage cybersecurity risks.
- The public comment period will remain open through May 9, after which the SEC will review and analyze the feedback received before adopting final rules, likely before the end of the year.
- While the proposed rules require only increased disclosures, not changes to cybersecurity risk management practices or board composition, the detailed and

prescriptive nature of the proposed disclosure requirements could signal the SEC's expectations about the design and operation of corporate cybersecurity programs, and could lead to a convergence of market practice and investor expectations around how companies manage and disclose their cybersecurity incidents, governance and risks.

- Public companies can begin preparing now for the potential new disclosure obligations, which may increase compliance costs and burdens, investor and regulatory scrutiny, and enforcement and litigation risks. Please engage with Gunderson Dettmer's public companies and data privacy teams to discuss actions you may wish to consider taking now in anticipation of final SEC rules.

Background and Overview

Last month, the SEC unveiled its highly anticipated rule proposal that would, for the first time, expressly mandate reporting by public companies about cybersecurity incidents, governance and risks, including (i) current and periodic reporting about material cybersecurity incidents (including updates about previously reported cybersecurity incidents) and (ii) annual reporting about a company's policies and procedures to identify and manage cybersecurity risks; management's role and expertise in assessing and managing cybersecurity risks and implementing related policies, procedures and strategies; and the board of directors' oversight role and any cybersecurity expertise. The proposed rules would apply to all SEC reporting companies with relevant disclosure obligations on Forms 10-K, 10-Q, 20-F, 8-K or 6-K, and proxy statements, including smaller reporting companies ("SRCs"), emerging growth companies ("EGCs") and foreign private issuers ("FPIs").

Since the start of his tenure, SEC Chair Gary Gensler has emphasized that cybersecurity rulemaking and enforcement would be one of the agency's top priorities. The rule proposal comes as cyberattacks have continued to grow in frequency, magnitude and sophistication over the last several years, affecting thousands of private and public sector entities—a trend accelerated by the pandemic-induced shift to remote work and increased reliance on digital technology to conduct and manage business. Costs and other adverse consequences arising from cyberattacks have continued to grow apace, and are estimated to run in the trillions of dollars per year in the U.S. alone. The SEC's rulemaking initiative has taken on new urgency in the wake of the Russian government's ongoing invasion of Ukraine, as federal agencies in recent weeks have warned U.S. businesses and senior corporate leaders of the heightened risk of Russian cyberattacks in reprisal for sweeping Western economic sanctions and export controls.[1]

The rule proposal also comes amid the Commission's intensified enforcement focus on public companies' cybersecurity disclosures and related controls and procedures. Most recently, in June and August of last year, the SEC settled cases and fined companies with deficient cybersecurity disclosures, inadequate cybersecurity disclosure controls and procedures, and disclosure of hypothetical cybersecurity risks when actual events had occurred.

In addition, a recent notable Delaware Court of Chancery decision involving a data security breach highlighted that "[c]ybersecurity has increasingly become a central compliance risk deserving of board level monitoring at companies across sectors." The court asserted that "as the legal and regulatory frameworks governing cybersecurity advance and the risks become manifest, corporate governance must evolve to address them. The corporate harms presented by non-compliance with cybersecurity safeguards increasingly call upon directors to ensure that companies have appropriate oversight systems in place."[2]

The SEC's proposing release highlights the ongoing and escalating risk that cybersecurity threats and incidents pose to public companies, noting that executives, boards of directors, investors and other market participants remain intensely focused on this issue. A 2019 survey cited by the Commission found that CEOs of the largest 200 global companies rated national and corporate cybersecurity as the number one threat to business growth and the international economy over the next 5-10 years. A 2021 survey of audit committee members identified cybersecurity as the second highest risk that their audit committee would focus on in 2022, second only to financial reporting and internal controls. The SEC also points to recent research suggesting that cybersecurity is among the most critical governance-related issues for investors, who it says have increasingly been seeking information about how (and how quickly) companies are detecting and remediating cybersecurity incidents and their associated risk management, strategy and governance practices.

Under the existing regulatory framework, there are no SEC disclosure requirements that explicitly refer to cybersecurity risks or incidents, and current cybersecurity practices vary widely across companies. Although the SEC acknowledged that companies' disclosures of both material cybersecurity incidents and cybersecurity risk management, strategy and governance practices have improved in terms of quality and frequency alike since the issuance of Commission-level cybersecurity guidance in 2018, which reinforced and expanded on the staff-level cybersecurity guidance published in 2011,[3] it noted that "current reporting may contain insufficient detail and the staff has observed that such reporting is inconsistent, may not be timely, and can be difficult to locate." It further expressed concern that material cybersecurity incidents may be underreported.

The proposing release describes a number of prevailing divergent cybersecurity reporting practices that the SEC believes frustrate investors' ability to assess and compare cybersecurity risk profiles across companies, including certain cybersecurity incidents that were reported in the media but not disclosed in SEC filings; differences in the timeliness of cybersecurity incident disclosures; varying levels of specificity provided regarding the cause, scope, impact and materiality of cybersecurity incidents and related remediation efforts; cybersecurity disclosures made in different sections of periodic and current reports, and sometimes blended with other unrelated disclosures; variations in approach to cybersecurity disclosures by industry; and a lower overall volume of cybersecurity disclosure provided by smaller companies as compared to larger companies.

To address these concerns, the new cybersecurity disclosure framework, if implemented as proposed, would substantially augment the Commission's existing principles-based guidance with a precise set of highly detailed and prescriptive mandatory disclosure rules. Specifically, the proposed rules would:

- Amend Form 8-K to add new Item 1.05 to require companies to disclose specified information about a material cybersecurity incident within four business days of determining that the incident is material (rather than within four business days of discovering the incident);
- Amend Forms 10-Q and 10-K to require companies (i) to provide disclosure of material changes, additions or updates relating to previously reported material cybersecurity incidents and (ii) to disclose, to the extent known to management, when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate, in each case as specified in proposed new Item 106(d) of Regulation S-K;
- Amend Form 10-K to require companies to disclose, as specified in proposed new Items 106(b) and (c) of Regulation S-K:
    - A company's policies and procedures, if any, for identifying and managing cybersecurity risks, including whether and how the company considers cybersecurity risks as part of its business strategy, financial planning and capital allocation;
    - A company's cybersecurity governance, including the board of directors' oversight role with respect to cybersecurity risk; and
    - Management's role, and relevant expertise, in assessing and managing cybersecurity risks and implementing related policies, procedures and strategies;

- Amend Item 407 of Regulation S-K to add new paragraph (j) to require companies to disclose, in annual reports and proxy statements involving the election of directors, whether any board members have expertise in cybersecurity and, if so, their names and a detailed description of the nature of their expertise; and

- Require that the proposed cybersecurity disclosures be presented in Inline XBRL.

In prepared remarks accompanying the proposal's release, Chair Gensler acknowledged that although many companies already provide cybersecurity disclosure to investors, "I think companies and investors alike would benefit if this information were required in a consistent, comparable and decision-useful manner."

The lone Republican commissioner voted against the proposal, writing in a dissenting statement that its detailed disclosure obligations represent "an unprecedented micromanagement by the Commission of the composition and functioning of both the boards of directors and management of public companies." "Such precise disclosure requirements look more like a list of expectations about what issuers' cybersecurity programs should look like and how they should operate," she argued, and "will have the undeniable effect of incentivizing companies to take specific actions to avoid appearing as if they do not take cybersecurity as seriously as other companies. The substance of how a company manages its cybersecurity risk, however, is best left to the company's management to figure out in view of its specific challenges."

The proposal is one of multiple policy projects the SEC is actively developing to bolster cybersecurity disclosures by regulated entities. In February, the SEC proposed rules that would impose significant new cybersecurity obligations on registered investment advisers and funds, and the agency is considering additional cybersecurity rulemaking applicable to broker-dealers and other financial firms.

The public comment period will remain open through May 9, after which the SEC will review and analyze the feedback received before adopting final rules, likely before the end of the year.

Material Cybersecurity Incident Reporting

Current Reports—Form 8-K Disclosure of Material Cybersecurity Incidents

Proposed Item 1.05 of Form 8-K would require companies to disclose the following information about a material cybersecurity incident within four business days of determining that the incident is material, to the extent known to management at the time of the filing:

- When the incident was discovered and whether it is ongoing;

- A brief description of the nature and scope of the incident;
- Whether any data was stolen, altered, accessed or used for any other unauthorized purpose;
- The effect of the incident on the company's operations; and
- Whether the company has remediated or is currently remediating the incident.

Companies would not be expected to publicly disclose specific, technical information about their planned response to the incident or their cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as could provide clues to malicious actors to better calibrate future attacks or as could otherwise compromise or impede their response or remediation efforts.

Definitions

"**Cybersecurity incident**" would be defined as "an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein."

"**Information systems**" would be defined as "information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of a registrant's information to maintain or support the registrant's operations."

The SEC notes that these proposed definitions are similar to those used in other federal cybersecurity rulemakings.

Examples

The proposing release notes that what constitutes a "cybersecurity incident" for purposes of the proposal should be construed broadly, and includes the following non-exclusive list of examples of cybersecurity incidents that would merit disclosure under Form 8-K Item 1.05 if determined to be material:

- An unauthorized incident that has compromised the confidentiality, integrity or availability of an information asset (data, system or network), or violated the company's security policies or procedures, stemming from either the accidental exposure of data or a deliberate attack to steal or alter data;

- An unauthorized incident that caused degradation, interruption, loss of control, damage to or loss of operational technology systems;
- An incident in which an unauthorized party accessed, or a party exceeded authorized access, and altered or has stolen sensitive business information, personally identifiable information, intellectual property or information that has resulted, or may result, in a loss or liability for the company;
- An incident in which a malicious actor has offered to sell or has threatened to publicly disclose sensitive company data; or
- An incident in which a malicious actor has demanded payment to restore company data that was stolen or altered.

Reporting Trigger

The reporting trigger for an Item 1.05 Form 8-K would be the date the company determines that a cybersecurity incident it has experienced is material, rather than the date it discovers the incident (though the two dates may coincide). The SEC notes it would expect companies to be diligent in making a materiality determination in as prompt a manner as feasible. To address any concern that some companies might delay making such a determination to avoid a disclosure obligation, Instruction 1 to proposed Item 1.05 states that **companies would be required to make a materiality determination regarding a cybersecurity incident "as soon as reasonably practicable after discovery of the incident."**

Materiality

What constitutes "materiality" for purposes of this disclosure would be consistent with the Supreme Court definition of materiality (i.e., information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available").[4]

To determine whether the cybersecurity incident is material, the SEC emphasizes that companies "would need to thoroughly and objectively evaluate the total mix of information, taking into consideration all relevant facts and circumstances surrounding the cybersecurity incident, including both quantitative and qualitative factors. Even if the probability of an adverse consequence is relatively low, if the magnitude of the loss or liability is high, the incident may still be material; materiality 'depends on the significance the reasonable investor would place on' the information."

No Reporting Delay

Proposed Item 1.05 would not allow for a reporting delay where there is an ongoing internal or external investigation (including law enforcement investigations) related to the cybersecurity incident or where the company would be excused from a reporting obligation under an applicable state or federal law delay provision. As a result, **there is a possibility that a company would be required to disclose a material cybersecurity incident under Form 8-K Item 1.05 even when it could delay reporting the incident under other applicable laws**.

Importantly, while the SEC recognizes that a delay in reporting may facilitate civil or criminal law enforcement investigations aimed at apprehending the perpetrators of the cybersecurity incident and preventing future cybersecurity incidents, the SEC believes, on balance, that any such delay provision would undermine the importance of timely and consistent disclosure of material cybersecurity incidents for investors. The SEC's prioritization of speedy disclosure above such other considerations could complicate companies' remediation efforts, and the conduct of investigations by law enforcement or other agencies that could reduce or eliminate the impact of the cybersecurity incident on the company and its stakeholders, and limit or prevent future impacts on others.

Consequences of Late Filings

As is the case with other Form 8-K disclosure items that require management to quickly assess the materiality of an event to determine whether a disclosure obligation has been triggered, the proposal provides that untimely disclosure of material cybersecurity incidents on Form 8-K would not result in the loss of Form S-3 eligibility and also would fall within the limited safe harbor from liability under Section 10(b) of the Securities Exchange Act of 1934 ("Exchange Act") and Rule 10b-5 thereunder.

- **Eligibility to Use Form S-3***.* The proposal would amend the general instructions to Form S-3 to add proposed Item 1.05 to the list of Form 8-K items that, if untimely filed, do not result in the loss of eligibility to use Form S-3 registration statements, so long as Form 8-K reporting is current at the time the Form S-3 is filed.

- **Limited Safe Harbor from Exchange Act Section 10(b) and Rule 10b-5 Liability***.* The proposal also would amend Exchange Act Rules 13a-11(c) and 15d-11(c) to include proposed Item 1.05 in the list of Form 8-K items that are eligible for a limited safe harbor from public and private claims under Exchange Act Section 10(b) and Rule 10b-5 in the event of an untimely filing.

Periodic Reports—Updated Cybersecurity Incident Disclosure in Forms 10-Q and 10-K

Updates to Previously Filed Form 8-K Disclosure

Proposed Item 106(d)(1) of Regulation S-K would require companies to disclose any material changes, additions or updates relating to previously reported material cybersecurity incidents on Form 8-K in a periodic report (Form 10-Q or Form 10-K for the fourth quarter) for the quarter in which the material change, addition or update occurred.

In order to assist companies in developing updated incident disclosure in their periodic reports, Proposed Item 106(d)(1) offers the following non-exhaustive examples of the type of disclosure that should be provided, if applicable:

- Any material effect, or potential material future impacts, of the incident on the company's operations and financial condition;
- Whether the company has remediated or is currently remediating the incident; and
- Any changes in the company's cybersecurity policies and procedures as a result of the incident, and how the incident may have informed such changes.

The SEC underscores that, notwithstanding the ability to provide updated incident disclosure under proposed Item 106(d)(1), there may be situations where a company would need to file an amended Form 8-K to correct disclosure from the initial Item 1.05 Form 8-K, such as where the original disclosure becomes inaccurate or materially misleading as a result of subsequent developments regarding the incident. For example, if the impact of the incident is determined after the initial Item 1.05 Form 8-K filing to be significantly more severe than previously disclosed, an amended Form 8-K may be required.

Disclosure of Cybersecurity Incidents That Have Become Material in the Aggregate

When a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate, proposed Item 106(d)(2) would require companies to disclose the same information as described above for the Form 8-K reporting of material cybersecurity incidents in a periodic report (Form 10-Q or Form 10-K for the fourth quarter) for the quarter in which the company determines the incidents are material in the aggregate. Therefore, companies would need to analyze related cybersecurity incidents for materiality, both individually and in the aggregate.

The SEC explains that, while such incidents conceptually could take a variety of forms, one example would be where a malicious actor engages in a number of smaller but continuous cyberattacks related in time and form against the same company and, collectively, they are either quantitatively or qualitatively material, or both.

Form 10-K Disclosure of Cybersecurity Risk Management, Strategy and Governance

Risk Management and Strategy

The proposing release observes that most companies that disclosed a cybersecurity incident in 2021 did not describe their cybersecurity risk oversight and related policies and procedures, and some companies provided only general disclosures, such as a reference to cybersecurity as one of the risks overseen by the board or a board committee. In order to elicit more consistent and informative disclosure regarding corporate cybersecurity risk management and strategy, proposed Item 106(b) would require companies to "disclose in such detail as necessary to adequately describe" their policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including, but not limited to:

- Operational risk (i.e., disruption of business operations);
- Intellectual property theft;
- Fraud;
- Extortion;
- Harm to employees or customers;
- Violation of privacy laws and other litigation and legal risk; and
- Reputational risk.

"**Cybersecurity threat**" would be defined as "any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity or availability of a registrant's information systems or any information residing therein."

The following eight specific disclosure topics are enumerated for discussion, as applicable:

- Whether the company has a cybersecurity risk assessment program and a description of any such program;

- Whether the company engages assessors, consultants, auditors or other third parties in connection with any cybersecurity risk assessment program;
- Whether the company has policies and procedures to oversee and identify the cybersecurity risks associated with its use of third-party service providers (including, but not limited to, those providers that have access to the company's customer and employee data), including whether and how cybersecurity considerations affect the selection and oversight of these providers and contractual and other mechanisms the company uses to mitigate cybersecurity risks related to these providers;
- Whether the company undertakes activities to prevent, detect and minimize effects of cybersecurity incidents and a description of any such activities undertaken;
- Whether the company has business continuity, contingency and recovery plans in the event of a cybersecurity incident;
- Whether previous cybersecurity incidents have informed changes in the company's governance, policies and procedures, or technologies;
- Whether cybersecurity risks and previous cybersecurity incidents have affected or are reasonably likely to affect the company's strategy, business model, results of operations or financial condition and, if so, how; and
- Whether the company considers cybersecurity risks as part of its business strategy, financial planning and capital allocation and, if so, how.

A company that has not established any cybersecurity policies or procedures would not be required to state explicitly that this is the case, or explain why not.

Governance

In order to improve investors' ability to understand how companies prepare for, prevent or respond to cybersecurity incidents, proposed Item 106(c) would require disclosure of a company's cybersecurity governance, including the board of directors' oversight role with respect to cybersecurity risk and management's role, and relevant expertise, in assessing and managing cybersecurity risks and implementing the company's cybersecurity policies, procedures and strategies.

Board Oversight

Under proposed Item 106(c)(1), disclosure about the board's oversight role would be required to include a discussion, as applicable, of:

- Whether the entire board, specific board members or a board committee is responsible for the oversight of cybersecurity risks;
- The processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic; and
- Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management and financial oversight.

Role of Management

Under proposed Item 106(c)(2), disclosure about management's role would be required to include, but not be limited to, the following information:

- Whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, specifically the prevention, mitigation, detection and remediation of cybersecurity incidents, and a detailed description of their relevant expertise;
- Whether the company has a designated chief information security officer (or someone in a comparable position) and, if so, to whom that individual reports within the company's organizational chart, and a detailed description of their relevant expertise;
- The processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection and remediation of cybersecurity incidents; and
- Whether and how frequently such persons or committees report to the board of directors (or a committee of the board) on cybersecurity risk.

Examples of relevant management expertise include prior work experience in cybersecurity; any relevant degrees or certifications; and any knowledge, skills or other background in cybersecurity.

Proxy Statement Disclosure of Board Cybersecurity Expertise

Proposed Item 407(j) of Regulation S-K would require, in annual reports on Form 10-K and proxy statements involving the election of directors, disclosure of whether any member of the company's board of directors has expertise in cybersecurity and, if so, the name(s) of such director(s) and a detailed description of the nature of their expertise. The proposed disclosure of "such detail as necessary to fully describe the

nature of the [director's cybersecurity] expertise" is not required about the board's audit committee financial expert.

This disclosure would be required in Item 10 of Part III of Form 10-K and thus would typically be disclosed in the company's proxy statement and incorporated by reference in Form 10-K.

"Cybersecurity expertise" is not defined, but the proposal provides the following non-exclusive list of criteria that companies should consider when determining whether a director has expertise in cybersecurity:

- Prior work experience in cybersecurity (e.g., as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner);
- Cybersecurity-related certifications or degrees; and
- Knowledge, skills or other background in cybersecurity (e.g., in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning).

A company that does not have a cybersecurity expert on its board would not be required to state expressly that this is the case, or explain why not.

Safe Harbor

Similar to audit committee financial experts, proposed Item 407(j) would include a safe harbor providing certain protections for a director who is identified as having cybersecurity expertise, including that such director would not be deemed an expert for any purpose, including for purposes of Section 11 of the Securities Act of 1933 ("Securities Act"), and such identification would not impose on such director any duties, obligations or liability that are greater than the duties, obligations and liability imposed on such director as a board member in the absence of such identification. Conversely, the identification of a cybersecurity expert on the board would not decrease the duties, obligations or liability of other board members.

Foreign Private Issuers

Because FPIs do not have Form 8-K filing obligations, the proposal would amend the general instructions to Form 6-K to include material cybersecurity incidents in the list of reporting topics that may trigger a Form 6-K filing. The proposal also would amend Form 20-F to add new Item 16J, which would require FPIs to provide the same type

of cybersecurity disclosures in their annual reports filed on that form as proposed to be required in periodic reports filed by domestic issuers under new Items 106 and 407(j) of Regulation S-K

Inline XBRL

The proposed cybersecurity disclosures would be required to be presented in Inline XBRL, including block-text tagging of narrative disclosures and detail tagging of any quantitative amounts disclosed within the narrative disclosures, in order to facilitate comparison and analysis of the information being disclosed.

Selected Issues for Public Input

Notable matters the SEC could address in the final rules, as reflected in the proposin release's specific requests for comment, include:

- Whether the SEC should modify or eliminate any of the specified cybersecurity incident disclosures in proposed Item 1.05, or require disclosure of any additional information about a material cybersecurity incident;
- Whether any of the proposed cybersecurity incident disclosures or the proposed timing of such disclosures could have the unintentional effect of putting companies at additional risk of future cybersecurity incidents;
- Whether the proposed four-business-day filing deadline would provide sufficient time for companies to prepare the required cybersecurity incident disclosures, or whether the SEC should modify the reporting timeframe;
- Whether the triggering event for the proposed cybersecurity incident disclosures should be the date the company discovers the cybersecurity incident rather than the date it determines the incident is material; or whether the SEC instead should require disclosure only if the expected costs arising from a cybersecurity incident exceed a certain quantifiable threshold (e.g., a percentage of the company's assets, equity, revenues or net income or, alternatively, a precise number);
- The extent to which the proposed Form 8-K incident reporting obligation would create conflicts for a company with respect to its other obligations under federal or state law;
- Whether delayed reporting of a cybersecurity incident should be allowed where the U.S. Attorney General requests such a delay based on their written determination that the delay is in the interest of national security;

- Whether, instead of requiring companies to file an Item 1.05 Form 8-K, the SEC should instead permit companies to furnish an Item 1.05 Form 8-K, such that the Form 8-K would not be subject to liability under Exchange Act Section 18 unless the company specifically states that the information is to be considered “filed” or incorporates it by reference into a filing under the Securities Act or Exchange Act;
- Whether the proposed definitions of the terms “cybersecurity incident,” “cybersecurity threat” and “information systems” are appropriate or should be revised, and whether it would be helpful to define the term “cybersecurity” (which is not defined in the proposal), for example as “any action, step, or measure to detect prevent, deter, mitigate, or address any cybersecurity threat or any potential cybersecurity threat”;
- Whether the proposed disclosures about cybersecurity risk management, strategy and governance would have the potential effect of undermining a company’s cybersecurity defense efforts or have other potentially adverse effects by highlighting a company’s lack of policies and procedures related to cybersecurity;
- Whether, as proposed, the names of board members with cybersecurity expertise should be required to be disclosed, and whether such a requirement would have the unintended effect of deterring persons with this expertise from serving on boards;
- Whether the term “expertise” in the context of cybersecurity should be defined and if so, how;
- Whether the proposed non-exclusive list of criteria a company should consider when determining whether a director has cybersecurity expertise is useful, and whether the list should be revised, eliminated or supplemented;
- Whether the proposed board cybersecurity expertise disclosure requirement would have the unintended effect of undermining a company’s cybersecurity defense efforts or otherwise impose undue burdens on companies and, if so, how; and
- Whether certain categories of issuers, such as SRCs, EGCs or FPIs, should be exempt from the proposed cybersecurity disclosure requirements or, alternatively, eligible for scaled disclosure accommodations, or for delayed compliance or other transition provisions.

What Companies Can Do Now to Prepare

While the proposed rules require only increased disclosures, not changes to cybersecurity risk management practices or board composition, the detailed and prescriptive nature of the proposed disclosure requirements could signal the SEC's expectations about the design and operation of corporate cybersecurity programs, and could lead to a convergence of market practice and investor expectations around how companies manage and disclose their cybersecurity incidents, governance and risks.

In anticipation of final SEC rules, public companies may wish to start a thorough review and assessment of their existing cybersecurity programs and protocols now, and consider taking some or all of the following actions:

- Conduct a thorough review of existing cybersecurity programs and controls.
- Implement and review robust vendor diligence and management programs.
- Engage third-party consultants or auditors to regularly review their cybersecurity risk management programs.
- Review and update all incident response protocols, including to reflect the proposed new disclosure obligations and timelines.
- Review governance and reporting structures at the board and management levels.

Related Materials

- Fact Sheet
- Proposed Rule
- Public Comment File

---

[1] The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency's (CISA) recent "Shields Up" guidance outlines a set of urgent cybersecurity focus areas and immediate actions for senior executives to ensure the security and resilience of their operations in the current heightened threat environment. See also the CISA-FBI Joint Cybersecurity Advisory to protect organizations from destructive malware used in Ukraine. On March 21, the White House issued a new warning urging private-sector businesses to take steps to harden their cybersecurity defenses immediately in light of "evolving intelligence that Russia may be exploring options for potential cyberattacks."

[2] *Firemen's Retirement System of St. Louis v. Sorenson (Marriott)*, 2021 WL 4593777 (Del. Ch. Oct. 5, 2021). Although the court did not allow the claims against the Marriott board to proceed, the language in the court's opinion is significant and suggests that cybersecurity could be considered to be a "mission critical" regulatory compliance risk for all companies and boards in certain contexts, which may subject directors to a *Caremark* claim alleging they violated their duty of corporate oversight (a breach of the duty of loyalty), potentially exposing them to personal liability.
[3] The 2011 and 2018 interpretive guidance was designed to assist companies in determining when they may be required to disclose information regarding cybersecurity incidents, governance and risks under existing disclosure rules (such as in risk factors, MD&A, description of business, legal proceedings or the financial statements), but imposes no prescriptive disclosure obligations. The 2018 guidance also addresses the importance of establishing and maintaining effective cybersecurity policies and procedures, including related disclosure controls and procedures, as well as the application of insider trading prohibitions in the cybersecurity context and the obligation to refrain from making selective disclosures of material nonpublic information related to cybersecurity incidents and risks before making full disclosure of that same information to the general public. The SEC notes the prior guidance will remain in effect regardless of whether the proposed disclosure requirements are adopted.
[4] See *TSC Industries, Inc. v. Northway, Inc.*, 426 U.S. 438 (1976); *Basic, Inc. v. Levinson*, 485 U.S. 224 (1988); and *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27 (2011).

Related Services

Data Privacy

Public Companies/Public Offerings

Featured Insights

FIRM NEWS

Gunderson Dettmer Commemorates 2025 Asian American and Pacific Islander Heritage (AAPI) Month

CLIENT NEWS

Brazilian Carbon Capture Company Mombak Announces $30M Financing

CLIENT NEWS

Africa B2B OmniRetail Announces $20M Financing

CLIENT NEWS

Glacier Announces Series A Financing to Expand Robot Recycling Fleet

CLIENT NEWS

Dataminr Announces $100M Investment Led by Fortress Investment Group

CLIENT NEWS

Omnidian Announces $87M Series C for Renewable Energy Performance

INSIGHTS

Splitting the Pie: How Savvy Founders Divide Ownership and Navigate Other Founder Equity Decisions

CLIENT NEWS

Chainguard Announces $356 Million Series D Led by Kleiner Perkins and IVP

INSIGHTS

Client Insight: California AI Transparency Act

INSIGHTS

Client Insight: Prepare for BE-10 Benchmark Survey of US Direct Investment Abroad

INSIGHTS

Tech Brew Interviews Aaron Rubin in “Where the legal battle stands around copyright and AI training”

CLIENT NEWS

Latin America Fintech Belvo Announces $15M Funding