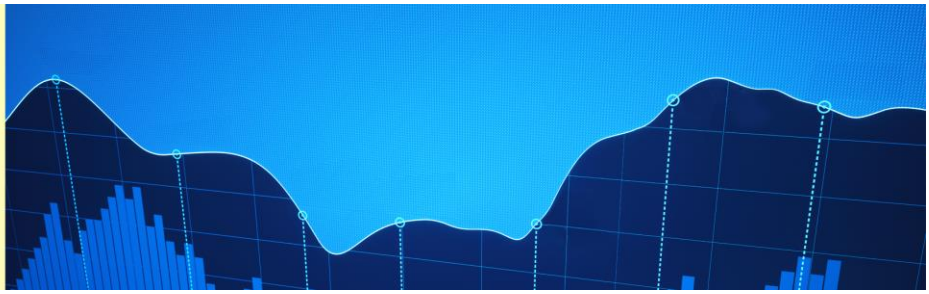
THOMPSON HINE



Securities Law Update

July 27, 2023

SEC Finalizes Rules Requiring Mandatory Cybersecurity Disclosure

On July 26 the SEC adopted final rules requiring certain cybersecurity-related disclosures, which were initially proposed in March 2022. The new rules are intended to "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance and incidents by public companies."

As adopted, the final rules differ in a number of ways from the proposal; among other areas, the SEC narrowed the scope of the cybersecurity incident-related disclosures in Form 8-K; provided that updated incident disclosures are required to be included on an amended Form 8-K, rather than Form 10-Q or 10-K; did not adopt proposed rules requiring disclosures of directors' cybersecurity expertise; and streamlined the proposed disclosure elements related to risk management. While many of these changes decreased the disclosure burdens compared to the proposed rules, many companies, particularly smaller reporting companies, may still find it costly and difficult to provide the required disclosures.

The varying obligations within the final rule will enter into force on a rolling basis, with the earliest requirements starting on December 18, 2023. Importantly, the SEC noted that the cybersecurity and data breach reporting obligations set forth in its rule are intended to "serve[] a different purpose" than the cybersecurity and data breach requirements being proposed by the U.S. Department of Homeland Security (DHS), and therefore the SEC's rule is not contingent on similar rulemaking being undertaken by DHS (or others in the federal government). Accordingly, organizations that are impacted by the final rule should immediately start updating their compliance programs.

Summary of New Rules and Effective Dates

Below is a summary chart provided by the SEC in the final release; see below under "New Disclosure Requirements" additional information regarding the new disclosures.

Item	Summary Description of Disclosure Requirement
Regulation S-K Item 106(b) – *Risk management and strategy*	Registrants must describe their processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats, and describe 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.
Regulation S-K Item 106(c) – *Governance*	Registrants must describe (i) the board's oversight of risks from cybersecurity threats, and (ii) management's role in assessing and managing material risks from cybersecurity threats.
Form 8-K Item 1.05 – *Material Cybersecurity Incidents*	Registrants must disclose any cybersecurity incident they experience that is determined to be material, and describe the material aspects of its (i) nature, scope, and timing; and (ii) impact or reasonably likely impact. An Item 1.05 Form 8-K must be filed within four business days of determining an incident was material. A registrant may delay filing as described below, if the United States Attorney General ("Attorney General") determines immediate disclosure would pose a substantial risk to national security or public safety. Registrants must amend a prior Item 1.05 Form 8-K to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8-K filing.

Annual disclosures will be required for annual reports on Form 10-K for fiscal years ending on or after December 15, 2023, and the Form 8-K requirements will become effective by the later of 90 days following publication of the release in the Federal Register or December 18, 2023. (Smaller reporting companies have an additional six months to provide the Form 8-K disclosures.)

Compliance Measures and Actions

Companies should begin preparing to comply with the new SEC disclosure requirements, which may include:

- strengthening their cybersecurity preparedness, hygiene and response by updating internal cybersecurity policies, including written information security plans;
- engaging in periodic tabletop exercises to test the effectiveness and efficiency of their incident response plans (IRPs);
- conducting data and asset mapping to identify and inventory key assets and data flows that may require elevated levels of protections;
- obtaining cybersecurity insurance or assessing adequacy of current cybersecurity insurance, and identifying carrier requirements for responding to a data security incident, including authorization to use breach counsel and digital forensic and incident response consultants;
- revising their internal disclosure controls and procedures and cybersecurity crisis management plans to address these new requirements, including incorporating the Form 8-K triggers and developing communication mechanisms within the company to address cybersecurity disclosure and insider trading blackout issues.
- updating their data security IRP to address the SEC's new reporting timelines and other requirements, including addressing "materiality" determinations, and periodically undertaking tabletop exercises to test its effectiveness and efficiency;
- assessing their current policies regarding public disclosure of cybersecurity incidents (for instance, some companies disclose incidents on Form 8-K even when they do not anticipate such incident will materially impact them);
- drafting tailored, specific disclosures for Form 10-K related to cybersecurity risk management, strategy and governance to comply with the new rules, including assessing board reporting structures and obtaining information regarding relevant expertise of management;
- reviewing other public disclosures, including risk factors, proxy statements and ESG reports, to ensure consistency in all public disclosures. (Risk factors should also include a description of any material cybersecurity incidents that occurred.); and
- implementing and maintaining a process to oversee third-party service providers that maintain business or proprietary data or provide key hardware or software, including employing due diligence mechanisms to assess the sufficiency and adequacy of the third party's information security program and imposing data breach response and liability obligations on the third party through contractual terms and conditions.

New Disclosure Requirements

New Item 1.05 Form 8-K

Companies will now be required to file an "Item 1.05 Material Cybersecurity Incidents" Form 8-K to report any material "cybersecurity incidents," which are defined as "an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a [company's] information systems that jeopardizes the confidentiality, integrity or availability of a [company's] information systems or any information residing therein." Accordingly, the SEC adopted a very broad definition that may be implicated by a wide range of cybersecurity attacks, including from network intrusion, data exfiltration, and extortion incidents to ransomware events that prevent access and use of key infrastructure or data.

Disclosure requirements. The Form 8-K is required to include (i) a description of the material aspects of the nature, scope and timing of the incident and (ii) the material impact, or reasonably likely material impact, of the incident on the company, including its financial condition and results of operations. Companies should consider both qualitative and quantitative factors in assessing whether an incident's impact is material, as "lack of quantifiable harm does not necessarily mean an incident is not material"; for example, harm to a company's reputation, customer or vendor relationships, or competitiveness, or the possibility of litigation or regulatory investigations or actions may constitute material or reasonably likely material impacts. However, companies are *not* required to disclose specific or technical information about their planned incident

response or their cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede their response to, or remediation of, the incident.

Another issue for companies to keep in mind is that cybersecurity incidents on a third-party system may trigger the required Form 8-K disclosure. According to the SEC rule, "[d]epending on the circumstances of an incident that occurs on a third-party system, disclosure may be required by both the service provider and the customer, or by one but not the other, or by neither." While companies should ensure they maintain regular contact with their third-party providers, the new rules "generally do not require that [companies] conduct additional inquiries outside of their regular channels of communication with third-party service providers pursuant to those contracts and in accordance with [companies]' disclosure controls and procedures." It is important for companies to delineate within their service provider contracts the data incident roles and responsibilities between the companies and their providers, including any notification and liability obligations. In addition, companies may consider requiring their service providers to periodically (e.g., quarterly, biannually) certify to them that they have not been subject to a material data security incident during the reporting period.

Timing of disclosures. The Form 8-K is generally due within four business days of determining that a cybersecurity incident is material. Following discovery of an incident, companies are required to determine whether such incident is material "without unreasonable delay." Although "without unreasonable delay" is not specifically defined, the SEC indicates that "a company being unable to determine the full extent of an incident because of the nature of the incident or the company's systems, or otherwise the need for continued investigation regarding the incident, should not delay the company from determining materiality." It also provides specific examples of what the SEC would consider an unreasonable delay, including intentionally deferring a board or committee meeting to determine materiality of an incident or revising existing policies or procedures to support delayed materiality determination or disclosure of the incident (e.g., extending incident severity assessment deadlines, changing the criteria that would require reporting an incident to internal management or committees).

In addition, if a company determines an incident is material, and information required by Item 1.05 is not determined or available at the time filing is required, the company must include a statement to that effect in its initial Form 8-K and file a Form 8-K/A disclosing such information within four business days after it determines such information or such information becomes available.

The Form 8-K filing may be delayed in certain specified instances, including when the U.S. Attorney General notifies the SEC in writing that it has determined that immediate disclosure would pose a substantial risk to national security or public safety and for companies complying with FCC rules regarding breaches of customer proprietary network information. The SEC expressly noted that it has established an interagency communication process with the Justice Department that is intended to allow for the U.S. Attorney General's determination to be communicated to the SEC in a timely manner. These breach notification exceptions are especially narrow and generally do not align with broader exceptions in state data breach notification requirements that allow for delays in incident reporting when such reporting would interfere with or impede a federal, state, or local criminal investigation or would be inconsistent with the legitimate needs of law enforcement agencies. Any failure to timely report an incident under Item 1.05 will not affect a company's eligibility to file a registration statement on Form S-3.

Effective date. Form 8-K Item 1.05 disclosure requirements will become effective as follows: (i) for non-smaller reporting companies, the *later* of 90 days following publication of the release in the Federal Register or December 18, 2023; and (ii) for smaller reporting companies, the *later* of 270 days following publication of the release in the Federal Register or June 15, 2024. **All** companies will be required to include iXBRL tags beginning on the *later* of 465 days following publication of the release in the Federal Register or December 18, 2024.

New Item 1C of Form 10-K

The SEC also adopted new Regulation S-K Item 106, which requires cybersecurity-related disclosures in companies' annual reports on Forms 10-K under a new "Item 1C. Cybersecurity."

Disclosure requirements. Under Item 106, companies will be required to describe, among other things:

- Their processes (if any) for assessing, identifying and managing material risks from cybersecurity threats, "in sufficient detail for a reasonable investor to understand those processes." Among other things, companies should address (i) whether and how any such processes have been integrated into their overall risk management system or process; (ii) whether they engage certain third parties in connection with such processes; and (iii) whether they have processes to oversee and identify such risks from cybersecurity threats associated with their use of any third-party service providers. Companies should also disclose information that is necessary, based on their facts and circumstances, for a reasonable investor to understand their cybersecurity processes. While the final rule does not include the specified risk types from the proposal (i.e., intellectual property theft, fraud, extortion, harm to employees or customers, violation of privacy laws and other litigation and legal risk and reputational risk), the SEC included them in the release as "guidance"; as such, companies should keep these risks in mind when drafting their disclosures.
- Whether and how 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 board of directors' oversight of risks from cybersecurity threats, including any board committee or subcommittee responsible for such oversight and the processes by which the board, committee or subcommittee is informed about such risks.
- Management's role in assessing and managing material risks from cybersecurity threats, including (i) if any management positions or committees are responsible for assessing and managing such risks, identifying such position(s)/committee(s) and their relevant expertise (which may include any cybersecurity-related prior work experience, relevant degrees or certifications, or knowledge, skills or other background); (ii) how such persons or committees are informed about and monitor the prevention, detection, mitigation and remediation of cybersecurity incidents; and (iii) whether such persons or committees report information about such risks to the board or a board committee or subcommittee.

Effective date. The Form 10-K Item 106 disclosure requirements will become effective for all companies beginning with annual reports on Form 10-K for fiscal years ending on or after December 15, 2023, or the 2023 Form 10-K for fiscal year-end companies. Companies will be required to include iXBRL tags beginning with annual reports for fiscal years ending on or after December 15, 2024, or the 2024 Form 10-K for fiscal year-end companies.

FOR MORE INFORMATION

For more information, please contact:

Jurgita Ashley
216.566.8928
Jurgita.Ashley@ThompsonHine.com

Steven G. Stransky
216.566.5646
Steve.Stransky@ThompsonHine.com

Julia Miller
216.566.5831
Julia.Miller@ThompsonHine.com

Thora Knight
212.908.3971
Thora.Knight@ThompsonHine.com

or another member of our Securities, Capital Markets & Corporate Governance or Privacy & Cybersecurity teams.