GUNDERSON DETTMER

Quick Reference Guide

New SEC Rules for Public Company Cybersecurity Risk Management, Strategy, Governance and Incident Disclosures

In July 2023, the SEC adopted final rules requiring enhanced and standardized disclosures related to cybersecurity for public companies, including emerging growth companies and smaller reporting companies. The final rules mandate **(1)** Form 8-K disclosure of material cybersecurity incidents within four business days of determining the incident's materiality and **(2)** Form 10-K disclosure of cybersecurity risk management, strategy and governance practices, including company cybersecurity risk management processes, and the roles of management and the board of directors in cybersecurity oversight and governance. The new rules supplement, but do not replace, the SEC's existing cybersecurity interpretive guidance (see 2011 guidance and 2018 guidance), which remains in effect and should be used to inform potential disclosure obligations not specifically addressed in the final rules. The most significant aspects of the final rules are summarized below. For detailed information on the new reporting requirements, please see the Gunderson Dettmer PubCo Insight.[1]

Form 8-K Disclosure of Material Cybersecurity Incidents (New Item 1.05 of Form 8-K)	
Compliance Date	• **December 18, 2023** for *all companies other than smaller reporting companies* • **June 15, 2024** for *smaller reporting companies*
Disclosure Content	Companies *MUST DISCLOSE* the following information about a material "cybersecurity incident" **within four business days after determining the incident is material**: • The **material aspects of the nature, scope and timing of the incident**; and • The **material impact or reasonably likely material impact on the company**, including its financial condition and results of operations. A company *NEED NOT DISCLOSE* "specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede [its] response or remediation of the incident."
Applicable Definitions	• "**Cybersecurity incident**" means "an unauthorized occurrence, *or a series of related unauthorized occurrences*, 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**" means "electronic 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 the registrant's information to maintain or support the registrant's operations."
Materiality Determination	Timing • Companies are required to make a materiality determination regarding a cybersecurity incident "**without unreasonable delay after discovery of the incident.**" • 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." Substance • A cybersecurity incident 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." • Companies should consider **qualitative factors** alongside **quantitative factors** when assessing materiality; a "lack of quantifiable harm does not necessarily mean an incident is not material."
Third-Party Incidents	Cybersecurity incidents on a third-party system (e.g., cloud-based or hosted systems) may trigger the required Form 8-K disclosure: "the materiality of a cybersecurity incident is contingent neither on where the relevant electronic systems reside nor on who owns them, but rather on the impact to the [company]."

[1] This is intended to be used as a quick reference guide only. As with any new rules, we will be monitoring how early filers respond, and will share insights on any developing disclosure trends. See also the SEC's Final Rule, related Fact Sheet and Small Entity Compliance Guide.

National Security/Public Safety Reporting Delay	Incident disclosure on Form 8-K may be delayed, initially for up to 30 days, if the U.S. Attorney General determines immediate disclosure would pose a "**substantial risk to national security or public safety**" and notifies the SEC of such determination in writing prior to the Form 8-K deadline. The delay may be extended for an additional 30-day period and (in extraordinary circumstances) for a final additional 60-day period in a similar fashion. To extend the delay beyond 120 days, the SEC must grant relief through an exemptive order.
Updating Previously Disclosed Incidents	To the extent that any required information about a material cybersecurity incident is not determined or is unavailable at the time the company prepares the initial Item 1.05 Form 8-K (e.g., regarding the incident's nature, scope or impact), the company must include a statement to this effect in the filing and then file a Form 8-K amendment containing such information within four business days after such information is determined or becomes available.
Aggregation of "Related" Immaterial Incidents	When a company concludes it has been materially affected by what may appear as a series of related cyber intrusions (e.g., involving the same malicious actor or exploitation of the same vulnerability), Item 1.05 may be triggered even if the material impact or reasonably likely material impact of each individual intrusion is by itself immaterial.
Safe Harbors	Untimely disclosure of material cybersecurity incidents on Form 8-K will *NOT* result in the loss of Form S-3 eligibility and will fall within the limited safe harbor from securities fraud liability under Exchange Act Section 10(b) and Rule 10b-5 thereunder.
Form 10-K Disclosure of Cybersecurity Risk Management, Strategy & Governance (New Item 106 of Regulation S-K)	
Compliance Date	**Annual reports for fiscal years ending on or after December 15, 2023** for *all companies, including smaller reporting companies* (meaning, for calendar-year-end companies, the fiscal 2023 Form 10-K filed in 2024)

Risk Management & Strategy
(Regulation S-K Item 106(b))
	Companies must disclose:
	• 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, including (as applicable):
	  ○ Whether and how the described cybersecurity 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;
	  ○ Whether the company has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider; and
	• 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.

Governance—Board Oversight ***(Regulation S-K Item 106(c)(1))***	Companies must describe the board of directors' oversight of risks from cybersecurity threats, including (as applicable): • The identity of any board committee or subcommittee responsible for such oversight; and • The processes by which the board or such committee is informed about such risks. ***The final rules dropped the proposed requirement to identify board-level cybersecurity expertise.***
Governance—Role of Management ***(Regulation S-K Item 106(c)(2))***	Companies must describe management's role, and relevant expertise, in assessing and managing material risks from cybersecurity threats, including (as applicable): • 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. 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.
Applicable Definition	"**Cybersecurity threat**" means "any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity or availability of a registrant's information systems or any information residing therein."