AUGUST 2023

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

SEC Issues Rules on Cybersecurity Reporting Obligations

On July 26, the Securities and Exchange Commission (SEC) issued new rules adding cybersecurity disclosures for public companies in three areas: cybersecurity incidents, governance, and risk management and strategy. The new rules require a company to (1) report material cybersecurity incidents within four business days and (2) include in their annual report information about how it manages material risks from cybersecurity threats and what role leadership plays in addressing cybersecurity issues. The obligations concerning breach reporting will take effect on December 18, while the disclosures about cybersecurity governance and strategy (along with risk management) must be included in annual reports for the first fiscal year ending after December 15.

Key Takeaways

- **Disclose cybersecurity incidents.** Report a material cybersecurity incident within four business days of determining the incident was material and update that filing as needed.
- **Share details on cybersecurity oversight.** Explain in your annual report how (1) your board of directors oversees cybersecurity threats and (2) management addresses material risks from cybersecurity threats.
- **Explain cybersecurity risks.** Disclose in your annual report your strategy for identifying/managing material risks from cybersecurity threats and explain how such risks have impacted the company.

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Josh Hansen
Associate
303.285.5306
jahansen@shb.com

Practical Tips

- **Focus on material risks.** Identify factors that will inform materiality determinations for cybersecurity threats ("materiality" here is the same standard articulated by the SEC and courts).
- **Document materiality determinations.** Ensure you have a process for recording why an incident is or is not material so that you can substantiate disclosure (or nondisclosure) decisions.
- **Revise incident response plans.** Update response plans to ensure stakeholders, including leadership, get necessary details to assess materiality without unreasonable delay.
- **Coordinate disclosures with CISO.** Work with your CISO to ensure disclosures are accurate but do not reveal confidential information that could imperil your response or defensive measures.
- **Review vendor oversight.** Verify that you have a robust assessment process for vendors to limit unflattering disclosures regarding (1) your oversight or (2) cybersecurity incidents affecting your vendors.

Colman McCarthy
Partner
816.559.2081
cdmccarthy@shb.com

Background

The SEC is promulgating the new rule against a backdrop of more than a decade of guidance. In 2011, the SEC's Division of Corporation Finance shared its view that "a number of disclosure requirements may impose an obligation on registrants to disclose such [cybersecurity] risks and incidents," even though "no existing disclosure requirement explicitly refers to [such issues]." The SEC offered more details in 2018 through interpretative guidance addressing the interplay between cybersecurity issues and existing disclosure requirements. But the lack of granular, cyber-specific requirements resulted in inconsistent disclosures.

In March 2022, the SEC set out to remedy the inconsistencies by proposing new rules explicitly requiring cybersecurity disclosures concerning governance, risk management, and incident reporting. The SEC explained new rules were necessary to ensure investors have "consistent, comparable, and decision-useful information" to evaluate companies' exposure to cyber risks/incidents and ability to manage those issues. This information, the SEC acknowledged, has become more critical because of the increasing (1) economic activity dependent on electronic systems; (2) number of cybersecurity incidents; and (3) costs and consequences of such incidents.

The SEC solicited comments on its proposed cybersecurity rules through May 2022 and then reopened the comment period in

October for two weeks due to technical glitches with the submission process. Following the SEC's spring 2023 meeting, the SEC indicated final action would come in October 2023. But they decided to not make us wait that long as the SEC published the final rule (along with a handy summary) at the end of July.

New Rule

The SEC's new rule adds disclosure obligations covering three cybersecurity topics: (1) incidents; (2) governance; and (3) strategy and risk management. For each topic, it is important to understand three key terms from the rule:

- **Cybersecurity Incident.** An unauthorized occurrence (or series of related occurrences) that jeopardizes the confidentiality, integrity, or availability of your IT systems, your vendor's systems, or the information stored on such systems. Yes, the rule covers incidents occurring at your vendors.

- **Cybersecurity Threat.** A potential cybersecurity incident—i.e., potential (or actual) unauthorized activity that jeopardizes your IT systems, your vendor's systems, or the data on those systems.

- **Materiality.** This is your general SEC standard—i.e., material facts are information that a reasonable shareholder would find important or view as significantly altering the total mix of available information. Considerations may include (among others): downtime, financial impact, reputational harm, litigation risks, and intellectual property losses.

Incident Reporting

The top line takeaway is that companies must file a Form 8-K (or 6-K for foreign companies) within four business days of determining a cybersecurity incident is material—and update the filing as needed. The filing must cover the material impact of the incident and material details about its nature, scope, and timing. The SEC states in the instructions that you do not need to address your response, IT systems, or vulnerabilities with a level of detail that would impede your response/remediation.

- **Trigger.** Conclude you experienced a material cybersecurity incident. A material incident can include (1) the cumulative effect of a series of incidents that, viewed in isolation, are immaterial or (2) a vendor incident affecting your data.

- **Content.** Explain the nature, scope, timing, and material impact (or reasonably likely material impact) of the incident. If any of those details are not known when you file, then you must acknowledge the omissions and update the response later as appropriate.

- **Updates.** Amend your 8-K when you obtain required information that was unavailable when you first filed the 8-K. Upon finding that new information, you have four business days to file an amended 8-K.

- **Timing.** Submit within four business days after determining the incident is material. Although this is not four days from when you discover the incident (nor necessarily four days after you complete the investigation), you must make the materiality assessment "without unreasonable delay" after discovering the incident. A company can delay their filing only if the U.S. Attorney General determines that disclosure "poses a substantial risk to national security or public safety" or the company must notify the Federal Communications Commission pursuant to its notification rule on customer proprietary network information.

- **Effective Date.** Companies must begin reporting under this rule by December 18, 2023 (although smaller reporting companies have until June 15, 2024).

The SEC slightly dialed back its original proposal following significant comments. The notable changes include (1) adding a limited delay for public/national security and (2) eliminating the requirement to discuss how remediation is progressing, whether data was affected, and whether the attack is still ongoing.

Governance

The critical takeaway here is that a company must include in its annual report information about how its (1) board of directors oversees cybersecurity threats and (2) management assesses and manages the material risks from such threats.

- **Content (Directors).** Explain how the board of directors oversees risks from cybersecurity threats and, if applicable, identify relevant committees and the process by which they are informed of cybersecurity threats.

- **Content (Managers).** Describe management's role in assessing and managing material risks from cybersecurity threats. This section should cover, at least: which groups are responsible for assessing/managing those risks, what relevant expertise the members possess, how those groups are informed about and monitor the company's cybersecurity strategy (prevention, detection, etc.), and whether those groups report to the board of directors.

- **Effective Date.** Companies need to start addressing cybersecurity governance in their first annual report for the fiscal year ending on or after December 15, 2023.

This section saw less changes in the final rule than the others. The SEC clarified companies only need to discuss management's role

for material risks from cybersecurity threats—not all risks. And the SEC also removed requirements to address (1) how the board integrates cybersecurity into its business strategy, risk, management, and financial oversight; (2) how often the board discusses cybersecurity; and (3) what cybersecurity expertise board members possess (but this requirement still exists for management).

Strategy and Risk Management

The key takeaway is that a company's annual report [10-K for domestic companies; 20-F for foreign companies] must address their cybersecurity strategy and how risks from cybersecurity threats have materially affected (or are reasonably likely to materially affect) the company.

- **Content (Strategy).** Describe your process for assessing, identifying and managing material risks from cybersecurity threats. At a minimum, this means covering: whether/how you integrate those processes into the larger risk management system, whether you engage third parties (such as auditors or consultants) for assistance, and whether you have processes to manage and identify threats arising from your use of vendors.

- **Content (Risk Management).** Explain what risks from cybersecurity threats have materially affected your company (or are reasonably likely to do so) and how those risks impacted the company. Considerations here may be issues such as business strategy, operations, and finances.

- **Effective Date.** Companies need to start addressing cybersecurity strategy and risk management in their first annual report for the fiscal year ending on or after December 15, 2023.

The SEC eliminated or narrowed certain requirements in the final rule to balance informing investors and limiting disclosures of sensitive details. There are three major changes. First, the new rule focuses on describing cybersecurity processes rather than policies/procedures. This limits the need to share more operational details that a threat actor could weaponize and invites a more holistic representation by no longer limiting the content to codified practices. Second, companies only need to describe their strategy for material risks rather than all risks. Third, companies no longer need to describe their (a) efforts to prevent/detect cybersecurity incidents; (b) continuity/response plans; (c) adjustments following prior incidents; or (d) cybersecurity assessments for (and oversight of) vendors.

The choice of a lawyer is an important decision and should not be based solely upon advertisements.