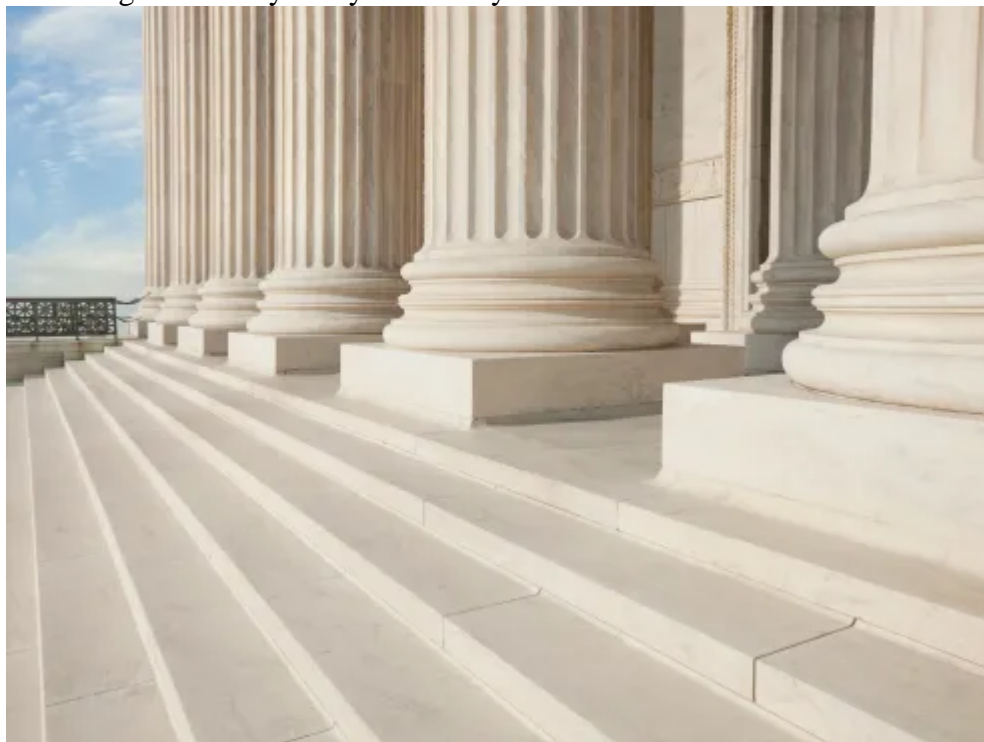


## [Articles](#)

September 18, 2023

### Updating Corporate and Cybersecurity Practices To Satisfy the SEC's Final Cybersecurity Disclosure Rules: Assessing Materiality of Cybersecurity Incidents



The U.S. Securities and Exchange Commission (SEC) announced the final version of its long-anticipated [cybersecurity rules](#) on July 26, 2023.

One new rule that will affect cybersecurity teams and executive management most directly requires covered companies to publicly disclose a "material" cybersecurity incident within four business days of determining that the incident is material.<sup>[1]</sup> Companies will have to comply with the rule beginning December 18, 2023.

The legal and reporting structures and requirements of the new rule are described in a [separate post](#), and some important aspects of making materiality determinations are described [here](#). But chief information security officers (CISOs), cybersecurity attorneys, and the executives and boards they advise require practical guidance on how to incorporate the new rule while planning for and conducting cyber incident response (IR).

Overall, the new SEC rule should be interpreted based on its purpose: to provide transparency and consistency of disclosure to investors about publicly traded companies. It is not designed to promote information sharing between companies, establish public-private partnerships, enhance law enforcement or national security efforts, mitigate cyber threats, or remediate cybersecurity incidents. The point is to inform the investing public.

Critically, complying with the new SEC rule is not simply a matter of providing sufficient information to satisfy legal requirements. Unlike most other federally mandated cybersecurity incident reporting, reports under the SEC rule must be *publicly available*. Four days after determining that an incident is material, a company must publicly describe what happened and the expected impact on the company. IR professionals are painfully aware that many aspects of an incident, including its technical and business impacts, may not be clear within such a short timeframe. As a result, while companies must make *sufficient* disclosures, they should also avoid making *excessive* disclosures or overcommitting to a conclusion. It is therefore important not only to conduct an informed materiality analysis, but also to limit the rapid, public disclosure to what the new rule requires.

Companies should distinguish between the new SEC rule and the [Cyber Incident Reporting for Critical Infrastructure Act of 2022](#) (CIRCIA). CIRCIA has different goals, contemplates a different and confidential reporting mechanism, and contains different thresholds—and has not been put into effect by regulations. The SEC may revise the new rule if a conflict with CIRCIA emerges, but CIRCIA should not currently factor into companies' reporting decisions under the SEC rule.

## Quick Vocabulary

Cybersecurity practitioners applying this guidance may be unfamiliar with the SEC's reporting terminology. Particularly relevant terms include:

- **Form 8-K.** [SEC form](#) for "current reports" that reporting companies must file to announce certain types of events (which the form lists) that shareholders should know about. These reports are filed promptly, in between companies' regular reporting.
- **Item 1.05.** Type of Form 8-K that requires disclosure of material cybersecurity incident.
- **Cybersecurity incident.** An "unauthorized occurrence" or a "series of related unauthorized occurrences" conducted on or through a company's information systems that jeopardizes the confidentiality, integrity, or availability (CIA) of the company's information systems or any information they contain. "Unauthorized" can include "accidental."
- **Material.** 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 to investors.
- **Information systems.** Electronic information resources owned or used by a company to process, maintain, use, share, disseminate, or dispose of the company's information to maintain or support company operations. Includes physical or virtual infrastructure controlled by such information resources or components thereof.<sup>[2]</sup>

The use of the term "jeopardizes" in the definition of "cybersecurity incident" caused concern among the public, but the SEC has noted that a cybersecurity incident only becomes relevant for the new rule's purpose if it has a material impact.

## When the Clock Starts

The *reporting* clock starts when a company determines that a cybersecurity incident is material, but compliance with the SEC reporting requirement really begins once the incident is discovered. The SEC will require companies to assess an incident's materiality "without unreasonable delay" after discovery. The SEC changed this phrasing from "as soon as reasonably practicable" to avoid putting undue pressure on companies to report before they have gathered sufficient information. The SEC has made clear that "a materiality determination necessitates an informed and deliberative process" but has also made clear that companies may not delay their materiality determinations to postpone the reporting deadline. The *assessment* clock therefore has no fixed period, but companies should expect their assessment process and timeframe to be scrutinized for reasonableness. Careful recordkeeping can help demonstrate after the fact that a company acted without unreasonable delay and made its materiality determination at an appropriate time.

Because the assessment period is used to develop information that bears on materiality, it can and should be used to clarify and memorialize the categories of information that the company will have to report.

If and when the assessment yields a determination that the incident is material, the *reporting* clock starts. Companies must use Form 8-K to report within four business days of that determination.<sup>[3]</sup>

### During the Assessment—Determining Materiality

The SEC explicitly declined to provide a materiality definition specific to cybersecurity events. Instead, the SEC directs companies to apply the long-standing definition of materiality that is used in securities law: 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** to investors.

Materiality is assessed from the perspective of a **reasonable investor** based on all relevant facts and circumstances. These include both **qualitative and quantitative factors**. As a result, the nature of affected data is as important as the amount of affected data.

Determinations regarding materiality will likely include, at minimum, a company's cybersecurity team, lawyers supporting that team, members of the C-suite, and securities attorneys. Whatever the composition of the team, it is crucial to focus on the impact of a potential cybersecurity incident on the company overall, and not to focus exclusively on "classic" cybersecurity questions.

Cybersecurity experts will have at least two roles. First, they will fulfill their familiar function of assessing the technical and direct consequences of a cybersecurity incident. That assessment alone may be sufficient to establish materiality. But their second function is to help the interdisciplinary team think more expansively about collateral ways in which the incident could materially affect the company.

For example, the SEC directs companies to consider "both the immediate fallout and any longer term effects" of an incident. Those effects include downstream effects on a company's operations, finances, brand perception, customer relationships, and other aspects of the business that may or may not be tangible or quantifiable. Reasonably foreseeable harm that may not occur immediately, but that may develop over time, must factor into the materiality analysis—such as harm from the theft of trade secrets or an undermining of consumer trust in a company's security.

Materiality determinations focus on the impact of an incident on the business and investors. As a result, a compromise of a third-party vendor such as a cloud service provider can constitute a material cybersecurity incident at a company if it has a sufficient effect on the company itself.

Based on the SEC's advice, an affected company and its IR team should incorporate the following guidance when assessing materiality:

- Take a **holistic** view of materiality.
  - Do not rely exclusively on quantitative thresholds.
  - Does the type of data affected create particular risk?
  - Does the type of system affected create particular risk?
  - Does a cybersecurity event have a direct impact on operations or the value of the company?
  - Does a cybersecurity event create downstream risk to the confidentiality, integrity, or availability of customer data or systems?
  - Does that event create longer-term risk for the value of the company?
    - Impact on competitiveness based on theft of intellectual property (IP) or customer lists.
    - Loss of customer confidence in privacy of information.

- Loss of customer confidence in security and/or continuity of operations.
  - Impact on reputation.
  - Impact on vendor relationships.
- Does the event expose a security flaw or other information that contradicts representations the company has previously made?
  - Does the fact or nature of the compromise expose the company to potential liability for prior statements, actions, or inaction regarding security?
- Does the event raise the likelihood of litigation, regulatory action, or investigations?
- A company can have sufficient information to determine that an incident is material **before an investigation is complete**. Possessing sufficient information makes the company responsible for making that determination promptly and starts the reporting clock.
  - A company should not wait to report until a full IR or investigation concludes if the company has sufficient information to make a materiality determination.
  - If "crown jewels" or key operational systems have been compromised, a company probably knows enough to make a materiality determination. This knowledge may well start the reporting clock even if a full investigation is not yet complete.
  - If an unauthorized actor has had access to or exfiltrated a large amount of important data, a company similarly probably has sufficient information to determine that an incident is material, and the reporting clock may start even if the full investigation is not yet complete.
  - The scenarios in the SEC release did not distinguish between encrypted and unencrypted data. Whether or not the affected data is encrypted, and whether or not an unauthorized actor possesses or obtains the key, will affect the materiality analysis but may not be dispositive.
- Although the SEC "streamlined" the substantive reporting requirements and imposed a short deadline, ensure that the report is **not misleading, including by omission**.
  - Legal and technical cybersecurity personnel in particular should probe IR teams' conclusions. For example, is a statement that a certain repository was not affected based on affirmative evidence, a lack of evidence, or inability to conduct analysis before the reporting deadline? If structured data fields were encrypted or otherwise protected, what about free text fields?
  - Identifying "known unknowns" in the initial report and filing an amended report once those gaps are filled is acceptable and contemplated by the new rule, as long as the review and determinations are not unreasonably delayed.
  - It is essential to file corrections—either of inaccurate statements or material omissions—promptly.
- When assessing whether an incident is material, following **"normal internal practices and disclosure controls and procedures"** will suffice to demonstrate good faith compliance."
  - A company should not change assessment or reporting criteria during an incident response for a purpose that appears to be delaying the required report.
  - If a board committee or other group must be convened to make the determination, a company should not defer or delay the meeting beyond the time it would usually take to convene the group.
  - For third-party incidents, there is no need to gather information outside of "regular channels of communication" with the relevant third-party service provider.
- Resolve doubt as to whether information is material **in favor of disclosure**.
- If a company is aware that reportable information has not been determined or is not available by the reporting deadline, it should **identify known gaps** in the report it files with the SEC and file an amended report when it has additional information.
- Do not assume that sharing threat information with private sector or government entities implies that a company has determined an incident to be material. The SEC clearly stated that alerting other parties of a threat does not in and of itself trigger a reporting obligation if the impact on the company is not material.

## Contents of the Report

The SEC's final rule "streamlined" the disclosure requirements to focus on "an incident's basic identifying details" and its material impact (or reasonably likely material impact) on the affected company. Accordingly, a report must describe "material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations."<sup>[4]</sup>

The SEC does not aim to require disclosure of details that threat actors could exploit. The new rule expressly does not contain a standalone requirement for "disclosure regarding the incident's remediation status, whether it is ongoing, and whether data were compromised." To the extent that details such as "data theft, asset loss, intellectual property loss, reputation damage, or business value loss" are material to the report, however, they must be included. A company is not required to "disclose specific or technical information about its planned response to the incident," its cybersecurity, or system vulnerabilities that would impede response or remediation.

### **Exceptions: Public Safety Delay, Classified Information, and Customer Proprietary Network Information**

The SEC only provides a narrow basis for delaying a report beyond the four-business-day deadline. The deadline can only be extended if the U.S. Attorney General finds that a disclosure would pose a substantial risk to national security or public safety. The basis for the finding can come from a different agency, so a local law enforcement or U.S. Intelligence Community agency, for example, can ask the attorney general to make the finding, but only the attorney general can authorize a delay in reporting. This process will likely be used rarely.

SEC rules already provided for the omission of classified national security information from public reporting. That provision applies to reporting under the new rule.

Finally, if a company suffers a breach of customer proprietary network information (CPNI) that is subject to the Federal Communications Commission (FCC) requirement to notify federal law enforcement seven days before disclosing the breach publicly, the company may follow the FCC rule with written notice to the SEC.

### **After Filing the Report or Determining That a Report Is Not Necessary**

Because of the short reporting timetable, it is possible that a company will develop additional reportable information, determine that additional information is reportable, or need to correct its report. New reportable information about an incident should be filed by amending the original report within four business days of the information becoming available or of the determination that it is reportable (presumably depending on why it was not included in the initial report). A company is not required to report *all* new information going forward; it only has to amend its original report with (1) new information that would have been called for in that original report; (2) information that has been newly determined to meet reporting requirements; (3) information correcting the original report; or (4) information addressing a material omission in the original report.

If a company investigates an event and determines that it is not a "cybersecurity event" under the SEC rule, the company may still have to report it later in time if the company determines that it is part of a "series of related unauthorized occurrences" that together have a material effect. Potential examples include small, continuous attacks from a single source or multiple attacks from multiple sources that exploit the same vulnerability. In either case, the impact of such attacks may only be material in the aggregate.

### **Incorporating Compliance With the SEC Rule Into IR Planning**

Companies should ensure that their substantive and procedural IR planning takes the new SEC reporting rule into account.

## **Substance**

Substantively, although the precise nature of a cybersecurity incident is impossible to predict, the interdisciplinary response team can develop factors that would help rapidly determine whether a future incident is material. A company's dependence on trade secrets, customer data, 24/7 availability of data and communications, cyber-physical controls, or logistics and inventory control, for example, is a good starting point for such analysis. Assess whether different types of compromises to different systems are likely to have a material impact on business. Existing practices of classifying information security events based on severity may be useful. So could developing a cyber "materiality matrix" that takes into account the impact of a cybersecurity incident. But the SEC is unlikely to look favorably upon companies that rely exclusively on applications of formulas to assess materiality. Any decisional frameworks should take into account both quantitative and qualitative effects of an incident and should build in consideration of incident-specific impacts.

Companies should also examine representations they have made about the security of their systems and data, as well as their compliance with applicable regulations and industry best practices. Beyond the reputational harm and impact on consumer confidence that a cybersecurity incident can cause, could a security incident reveal inaccuracies in a company's prior public statements? Has the company made commitments to regulators, litigants, shareholders, customers, or other constituencies, whether in the United States or overseas, that a cybersecurity incident could call into question? Will scrutiny of the company's security posture reveal a deficiency that adopting best practices would have corrected earlier? How will different constituencies—consumers, shareholders, regulators, and litigants—react?

These are questions that cybersecurity or IR professionals cannot answer on their own. Executives and counsel with a broad view of the company and a nuanced understanding of materiality (and relevant case law and enforcement actions) must participate in IR planning.

## **Process**

The need for interdisciplinary work to assess materiality raises questions of process. Given the short deadline the SEC has imposed and its warnings about undue delay, it is critical for companies to incorporate into their IR plan a workstream with deadlines to assess materiality and prepare a report if needed.

The "SEC workstream" should consist of a group that is small enough to work quickly and efficiently, but representative enough to provide the necessary interdisciplinary analysis. Most companies already have "disclosure committees" that meet to address other public disclosures the companies make in SEC filings, but a cybersecurity incident requires additional expertise that those on the disclosure committee might not have that are necessary to make the materiality determination.

The IR plan should identify core members (such as executive, legal, and cybersecurity representation) and specific points of contact from additional parts of the company who can be brought in as needed based on the nature of an incident. Assessing materiality is a legal obligation and involves legal analysis and advice, so limiting distribution and maintaining confidentiality of the workstream's deliberations will be important considerations to support any future claim of attorney privilege.

The "SEC workstream" group (including the core group and additional points of contact [POCs]) must remain engaged after the company files the initial report to address any gaps the report identified and ensure that material misstatements or omissions in the initial report are reported promptly in an amended report. Everyone involved must understand that they are both encouraged and required to flag new facts or analysis that may supplement—or even contradict—the initial report. For example, an observation stating, "We reported X based on facts available to us, but now that may not be accurate" may be one of the most important contributions a

team member can make as IR efforts proceed beyond the initial reporting date. A company must subject such observations to a materiality analysis under the substantive criteria, interdisciplinary approach, and procedural timetable discussed above.

As noted above, event classification schemes and decision matrices have important roles in assessing materiality, and they should reflect input from executive, operational, legal, cybersecurity, marketing, financial, human resources, research and development, and other perspectives as appropriate to a specific company.

The SEC's inclusion of aggregated incidents within the reporting requirement presents a process challenge. Information security teams probably already triage events to determine whether they bear similarities to other events, such as tactics, malware, or vulnerabilities. Because individual events that do not trigger an all-out IR process will likely only be noticed by security personnel, they need to be made aware of the need to identify a series of related events, and they must be responsible for flagging such a series to their management. Training and periodic reminders will be critical. A company should have a process for evaluating the materiality of such a series that similarly leverages all relevant disciplines and applies the same criteria discussed above. Those with questions about how the new cybersecurity disclosure guidelines should contact experienced counsel.

## Endnotes

[1] This note focuses on assessing materiality and reporting material cybersecurity incidents. It does not address whether the new SEC rule applies to a particular company and does not discuss other new SEC requirements related to cybersecurity that are not related to specific incidents.

[2] Operators of cyber-physical or other critical infrastructure should note that the SEC rule does not use the term "operational technology." We recommend reading the inclusion of infrastructure controlled by information resources in the definition of "information systems" to incorporate operational technology. See [Final Rule](#) at 81.

[3] The SEC adopted rules that make disclosures eligible for limited safe harbor treatment under securities laws because of the rapid timeframe for making materiality determinations. [Final Rule](#) at 39-40.

[4] [Final Rule](#) at 29; SEC Form 8-K Item 1.05(a). Note that The SEC will require companies to tag disclosures in Inline XBRL, "including by block text tagging narrative disclosures and detail tagging quantitative amounts." [Final Rule](#) at 88-89.

© 2023 Perkins Coie LLP

## Authors

## Explore more in

[Privacy & Security](#) [Ethics & Compliance](#) [Data Security Counseling and Breach Response](#)