Articles + Publications | July 19, 2024

Cyber Incident Response Checklist for SEC Compliance

WRITTEN BY

David I. Meyers | Sadia Mirza | Casselle Smith | Edgar Vargas

Published in Law360 on July 18, 2024. *© Copyright 2024, Portfolio Media, Inc., publisher of Law360. Reprinted here with permission.*

By now, public companies are generally aware of the cybersecurity rules adopted by the U.S. Securities and Exchange Commission a year ago, requiring public companies to disclose material cybersecurity incidents under Item 1.05 of Form 8-K.

More recently, on May 21, the SEC staff issued further guidance to clarify the distinction between two types of Form 8-K disclosures: Item 1.05, which should be used to disclose material cybersecurity incidents, as required under the disclosure rule; and Item 8.01, which may be used to disclose "other cybersecurity incidents" for which "it's too early to tell" whether the incident is material.

This new guidance is an attempt by the SEC to address the influx of Item 1.05 disclosures, with some pertaining to incidents deemed to be material and others falling in the "it's too early to tell" category. As of June 1, 24 companies filed such disclosures.

As companies continue to refine their materiality assessment processes, they should also reevaluate the relationship between their incident response processes and disclosure controls. If done well, the alignment of these processes can reinforce compliance with the SEC's disclosure rule and provide a measure of protection in the event of an SEC enforcement action.

While there is no one-size-fits-all approach to assessing materiality, evaluating existing processes against the questions set forth below may help companies avoid common pitfalls and improve the narrative around their response to and disclosure of material cybersecurity incidents.

Understanding your incident response team's triage process: Have you evaluated which incidents will be escalated and when?

The initial step in any effective materiality assessment process must involve the correct identification and escalation of incidents that require a review for materiality. Historically, security teams have implemented a process to triage incidents, which often involves assigning an incident severity level on a scale from 1 to 4 — with Level 1 being routine incidents manageable by internal IT members without further escalation, and Level 4 being major events requiring a comprehensive response.

Companies can leverage this triage process to identify the categories of incidents that should trigger a materiality assessment.

However, because these historic processes may not have been designed with materiality in mind, the security team should work with senior leadership and disclosure committee representatives to ensure the classification structure properly accounts for the factors that could affect materiality. The incident response team must be integrated into this process and trained to understand the types of incidents that should trigger the materiality assessment workflow.

In addition to facilitating transparency between the security team and leadership, these proactive discussions will also help support a culture of cybersecurity, where stakeholders understand that cybersecurity is not just a security issue.

Moreover, companies should work to foster a culture of compliance in which the security team is empowered to work collaboratively with the necessary internal and external stakeholders to achieve an appropriate and defensible incident response.

Among other things, failure to timely disclose a material cybersecurity incident can trigger a securities law violation, particularly when the nature of the delay implicates or involves security leaders.

Instead of striving for the unattainable goal of perfect or impenetrable cybersecurity, senior leadership should (1) be transparent that it is impossible to avoid all cybersecurity incidents or risks, and (2) emphasize that failure to properly escalate incidents internally in accordance with established protocols to facilitate a proper response is unacceptable.

The goal of these proactive discussions is to alleviate employees' fears of reprisal should the inevitable occur, thereby reducing the likelihood that certain teams or employees will attempt to conceal or address incidents in isolation.

Is your incident response team trained to document the notification process to leadership once an incident is escalated?

One of the first questions a regulator may ask following a cybersecurity incident is, "Who was notified and when?" Public companies must be prepared for the SEC to closely scrutinize the level of senior leadership's oversight and involvement in the company's response to a material incident.

As a threshold matter, companies should proactively discuss how such notifications will be provided and consider backup mechanisms if operations are down — e.g., email is no longer functioning — or if a particular leader or board member is unavailable. Planning for the logistics around communications in advance will prevent last-minute scrambling during a crisis.

Additionally, incident response teams and internal disclosure committees should be trained to maintain an accurate timeline that identifies who is notified — both internally and externally — about cybersecurity incidents. This timeline should include the notification method, e.g., conference call, dedicated cybersecurity bridge, in-person

meeting, etc., the timing of such notice, and how often updates were subsequently provided.

The golden rule of incident response: Does your materiality assessment process emphasize fact-based assessments and discourage speculation?

The golden rule of incident response has always been to rely on facts and avoid speculation to provide a solid foundation for decision making during incident response, effectively guiding the company's actions and strategies. This principle is crucial to manage litigation risk and avoid unnecessary reputational harm.

Not only can documentation and materials prepared during incident response often become evidence in subsequent litigation and investigations, but speculation can lead to inaccurate messaging during incident response efforts that the business must later correct.

Similarly, the information shared with the company's disclosure committee members should be grounded in confirmed facts — not speculation — to allow for accurate, reliable and defensible materiality assessments. Disclosure committees should also be trained and consistently reminded to base their assessments on verified facts.

Indeed, hastily deeming an incident as material based on a gut reaction and then attempting to retract that determination later could have negative repercussions for the organization, including reputational damage.

Disclosure statements relating to material cybersecurity incidents are expected to describe the material aspects of its nature, scope and timing, as well as its effect or potential effect.

By way of example, if you know that you will never be able to tell the full scope of an incident because forensic artifacts do not exist, the disclosure committee should be made aware of and have an opportunity to consider the implications of that fact. The disclosure committee may need the incident response team's assistance in determining the relevance and potential effects of the verified facts as they develop.

Collaborating closely with external counsel, from both a cybersecurity and disclosure standpoint, is also advised to ensure that disclosures do not inadvertently subject the company to avoidable liability or risk.

Not a one-and-done exercise: Do existing processes adequately capture materiality assessments as being an iterative process and create a culture of cybersecurity within the organization?

Facts develop rapidly during incident response, so it's crucial for companies to understand that materiality determinations are not a one-and-done exercise. Materiality assessments should be an iterative process, and companies should emphasize the importance of ongoing reviews of facts as they unfold.

To that end, the incident response team and disclosure committee should maintain a consistent and open communication channel to allow for communications in real time and reduce the need to wait for formal incident-related summaries or reports.

Incident response teams should be trained to reevaluate and validate their initial triage as the incident details

unfold. For example, it is not unusual for an incident initially classified as Level 2 to escalate to Level 3 as more information comes to light. If a company's protocols for assessing materiality are only triggered upon identifying a Level 3 incident, a procedural gap could arise if the incident response team is not trained to reclassify incidents as needed.

The process of assessing materiality does not conclude with the filing of a Form 8-K. The SEC acknowledges that as investigations advance, new information may emerge. Consequently, disclosure committees must consider new data that may surface as the investigation evolves. The SEC instructs registrants to submit an amendment within four business days to detail information not initially available or determined at the time of the original filing.

Is your process aligned with the recent SEC guidance on disclosing "other cybersecurity incidents"?

There are material cybersecurity incidents, and then there are "other cybersecurity incidents." Once a company determines a cybersecurity incident as material, it has four business days to disclose the incident under Item 1.05 of Form 8-K.

As recently as May 28, companies have disclosed nonmaterial cybersecurity incidents under Item 1.05 of Form 8-K. The SEC's recent guidance clarifies that, while companies are encouraged to voluntarily disclose incidents deemed nonmaterial, such disclosure should be made using a different item of Form 8-K, such as Item 8.01.

The SEC clarified that while voluntary disclosures are important for the market and investors, "it could confuse investors if companies disclose either immaterial cybersecurity incidents or incidents for which a materiality determination has not yet been made under Item 1.05."

Companies should incorporate this guidance into their existing assessment processes, as it is likely that it may not always be apparent whether an incident is material, especially at the outset of the investigation. Accordingly, companies should reference the potential use of Item 8.01 to disclose a cybersecurity incident for which they have not yet made a materiality determination or a cybersecurity incident that the company determined was not material.

Importantly, the SEC has indicated that if a company discloses a nonmaterial incident, or one for which it has not yet made a materiality determination, under Item 8.01 and then later determines that the incident is material, the company should file an Item 1.05 within four business day of such subsequent materiality determination. This later notice may reference the Item 8.01 initial notice, but should still satisfy the disclosure requirements of an Item 1.05 filing.

Does your materiality assessment process and incident response plan account for selective disclosure issues?

During incident response, companies often communicate with various stakeholders, including employees, business partners, vendors and customers. This communication can take the form of proactive statements concerning the detection of the incident and the company's response, FAQs, talking points, and regular updates concerning factual and forensic findings.

For public companies, it is crucial to ensure communications are consistent with the company's then-current stance on the incident's materiality. For instance, if the materiality of an incident is undetermined, any communication about the incident should avoid implying otherwise. Indeed, doing so could raise questions about the company's materiality assessment processes, particularly if the company has disclosed enough information through traditional incident response channels to identify the incident as material.

Communications should also be evaluated in light of the SEC's Regulation Fair Disclosure, which mandates that when a public company discloses material nonpublic information to certain individuals or entities — typically, securities market professionals or holders of the issuer's securities who might trade based on the information — the issuer must publicly disclose that information.

In the context of incident response, it's essential to work closely with external cybersecurity and SEC counsel to ensure that efforts to mitigate incident response risks on one hand do not inadvertently intensify SEC-related risks on the other.

Has the company integrated insider trading concerns into its incident response strategy?

As companies fine-tune their materiality assessment processes, they should consider potential insider trading issues once a cybersecurity incident occurs. Specifically, companies need to implement the proper protocols to guard against corporate insiders taking advantage of the period between (1) the company's discovery of a cybersecurity incident and (2) public disclosure of the incident to trade on material nonpublic information about the incident.[1]

These protocols should apply not just to those incidents deemed to be material, but also to other cybersecurity incidents, for which a determination has not yet been made. Guardrails should be in place to limit such trading, at least not without prior review and approval.

Does the company's materiality workflow account for updating prior risk factors and disclosures?

Once a company determines that a material cybersecurity incident has occurred, it is important to review prior risk factors and disclosures to ensure there are no statements suggesting otherwise.

For instance, if a company's SEC filings outline potential challenges and adverse conditions that could arise from such an incident, an investor reviewing these risk factors might incorrectly assume that no incident has occurred if the disclosures are not updated.

Ensuring that disclosures accurately reflect the current situation helps maintain transparency and prevents misleading investors about the company's cybersecurity status.

---

[1] See Statement and Interpretive Guidance 2018 pg. 5 (https://www.sec.gov/files/rules/interp/2018/33-10459.pdf).

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber