Articles + Publications | August 28, 2024

6 Considerations to Determine if a Cyber Incident Is Material

WRITTEN BY

Sadia Mirza | David I. Meyers | Jay A. Dubow | Ronald Raether, Jr. | Casselle A.E. Smith

Published in Law360 on August 28, 2024.

In late June, the staff of the U.S. Securities and Exchange Commission's Division of Corporation Finance released five new compliance and disclosure interpretations regarding the disclosure of material cybersecurity incidents under Item 1.05 of Current Reports on Form 8-K, specifically in situations involving ransomware payments.[1]

These cybersecurity compliance and disclosure interpretations provide guidance on materiality determinations when a company makes a ransomware payment to a threat actor, resulting in the business becoming fully operational and recovering its data.

These compliance and disclosure interpretations also explore scenarios where a company makes a ransomware payment but later recovers the payment amount through its cyberinsurance policy, as well as situations where a ransom payment is so minimal that it has no significant financial impact on the company.

The staff makes one underlying theme clear throughout this guidance: No single factor is determinative of whether a cybersecurity incident is material. Once a cybersecurity incident is determined to be material, however, it must be reported within four business days after the company determines that it has experienced a material cybersecurity incident.

The payment of a ransom demand or the outcomes that follow do not alter the assessment or Item 1.05 Form 8-K reporting requirement. Companies that take the opportunity to review the guidance now, before facing the pressures of an active ransomware attack, would be wise to reassess their materiality determination processes and implement these guardrails to ensure they are not overlooked when an actual incident occurs.

For businesses experiencing a ransomware attack and contemplating whether the cybersecurity incident is material, consider the following points.

1. Returning to normal business operations does not relieve a company of the requirement to make materiality determinations.

One of the primary objectives for a company following a ransomware attack is to get the business back up and

running safely and securely. Every day the business is not operational translates to financial loss, reputational harm and other deleterious impacts.

Achieving this often requires significant effort, including assistance from third-party restoration firms, rebuilding systems from scratch, and sometimes even negotiating with the threat actor for a decryption key in exchange for a ransom payment. Once the business is operational again, it is considered a significant win.

However, the staff's guidance urges caution. Returning to normal business operations does not absolve a company from the requirement to make materiality determinations.

Even if the company manages to restore operations in record time, it must still assess the materiality of the cybersecurity incident and report the incident under Item 1.05 of Form 8-k within four business days after the company determines that it has experienced a material cybersecurity incident.

On a positive note, if operations are restored quickly, it may indicate that the financial impact was minimal, which is a factor to consider when determining materiality.

The key point, according to the guidance, is that in assessing the materiality of the incident, a company should determine whether "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," regardless of the resolution of an incident, including if such resolution occurred because the company ultimately paid a ransom demand.

2. The return of data by a threat actor does not relieve a company of the requirement to make materiality determinations.

Ransomware attacks often result in files, folders and possibly entire systems becoming inaccessible due to encryption or deletion by the threat actor. In these cases, businesses frequently are forced to negotiate with the threat actor to have their data returned or unencrypted.

The compliance and disclosure interpretations clarify that, similar to how returning to normal business operations does not relieve companies of the requirement to make materiality determinations, neither does the return or recovery of data. Nevertheless, companies should still consider how the recovery of data affects their materiality assessment.

Indeed, a business that suffers permanent data loss is in a markedly different position from one that recovers all or part of its data, or from a business that recovers the data but must contend with any subsequent corruption issues.

A company should consider this factor when determining materiality, but the staff's point is clear: consider it as a factor, but do not assume that recovering data means the incident is no longer material or that a materiality assessment is no longer required.

3. Once an incident is deemed material, paying a ransom does not reverse that determination.

The staff explored a hypothetical scenario where a company determines that a ransomware attack involving operational disruption and data exfiltration is material. Following this determination, the company makes a ransomware payment to the threat actor, resulting in the business returning to normal operations and the return of its data.

The staff clarified that because the incident was already deemed material, the subsequent ransomware payment and resolution of the incident does not relieve such company of the requirement to report the incident under Item 1.05 of Form 8-K within four business days after determining that it has experienced a material cybersecurity incident.

From a practical perspective, companies should exercise caution when documenting their materiality assessment thought processes and conclusions. Importantly, personnel should be trained not to document any opinions or speculations on the materiality of incidents, as such documentation could be used against the company if later discovered.

It is crucial to remember that once a cybersecurity incident is determined to be material, the Item 1.05 Form 8-K reporting obligation is arguably triggered, and the company may have limited ability to argue otherwise.

Therefore, it is critical for companies to ensure they have effective policies and practices to ensure that any materiality determinations are thoroughly vetted, approved, and based on all available facts known at the time of such determination.

Companies would also be wise to discuss with appropriate level personnel the factors that ultimately resulted in any final determinations, providing opportunities to weigh in and discuss. This can prevent instances where the company makes a determination, but an employee disagrees.

Situations like this may result in whistleblower complaints, which could be prevented through open discussions and a clear understanding of roles and obligations, both at the employee and company level.

4. Insurance coverage for ransom payments is a consideration, not a determinative factor.

Continuing with the theme that no single factor is likely to be determinative of whether an incident is material, the compliance and disclosure interpretations clarify that if a company makes a ransomware payment and that payment, or a substantial portion thereof, is covered by such company's insurance policy, this alone does not mean that the incident is not material.

The key question, according to the guidance, remains whether "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."[2]

In this context, the compliance and disclosure interpretations clarify that companies "should take into consideration all relevant facts and circumstances, which may involve consideration of both quantitative and qualitative factors" including, for example, "consider[ing] both the immediate fallout and any long term effects on its operations, finances, brand perception, customer relationships, and so on, as part of its materiality analysis."

Relevant to this specific fact pattern, the compliance and disclosure interpretations indicate that insurance covering the ransom may affect the company's ability to obtain cyberinsurance in the future or, if still possible, may increase the cost of such insurance. These types of considerations must be factored into the materiality analysis.

5. The size of a ransomware payment by itself is not determinative, but consider long-term impact.

At this point, it should come as no surprise that the size of the ransomware payment, by itself, is not determinative as to whether a cybersecurity incident is material. In support of this position, the compliance and disclosure interpretations cite to the commission's statement in Item 1.05's adopting release, which indicated that:

[T]he material impact of an incident may encompass a range of harms, some quantitative and others qualitative. A lack of quantifiable harm does not necessarily mean an incident is not material. For example, an incident that results in significant reputational harm to a registrant … may not cross a particular quantitative threshold, but it should nonetheless be reported if the reputational harm is material.[3]

This underscores the importance for companies to consider the long-term impact of cybersecurity incidents. Often, a company can recover from a ransomware attack with little to no financial loss, even if a significant volume of data was taken, or possibly taken, by the threat actor.

For instance, a company with robust IT backups may not need to pay the threat actor, as it can recover without a decryption key and may choose not to pay for a promise from the threat actor to delete the data.

Even in such cases, however, the company may trigger breach notification obligations that attract media attention, customer issues, potential litigation and regulatory scrutiny. Thus, while the company may avoid a financial hit from the ransom payment, the company should consider the other repercussions from the incident.

6. Multiple cyber incidents over a period of time could be material if determined to be related.

The staff presents a hypothetical scenario involving a company that experiences "a series of cybersecurity incidents involving ransomware attacks over time, either by a single threat actor or by multiple threat actors."

While this hypothetical company appears to have other, not necessarily bigger, problems, one task added to its plate by the staff is determining whether the series of cybersecurity incidents are related. If such cybersecurity incidents are determined to be related, the compliance and disclosure interpretations clarify that such company should assess, collectively, whether those incidents were material.

When does the staff consider separate cybersecurity incidents to be related? The compliance and disclosure interpretations refer to the adopting release for Item 1.05, which provides two examples: (1) when the same malicious actor engages in a number of smaller but continuous cyberattacks related in time and form against the same company; or (2) when there is a series of related attacks from multiple actors exploiting the same vulnerability and collectively impeding the company's business materially.

If a company finds itself in this unfortunate situation, it would be prudent to determine whether there is a common

thread linking certain cybersecurity incidents.

This could be identified through common threat actor tactics, techniques and procedures, indicators of compromise, or other intelligence suggesting that the same threat actor or exploit is involved.

Where there is no common link, documenting the facts relating to each incident is critical, especially if the company determines that, while these incidents are not material individually, they would be material collectively if deemed related.

Conclusion

Companies that fall victim to ransomware attacks are immediately forced to navigate various different and overlapping workstreams.

Beyond the materiality issues discussed here, they must also balance efforts related to restoration; investigation; threat actor negotiations; decisions on whether to pay the ransom; determining file access or acquisition; ensuring compliance with Office of Foreign Assets Control regulations and the legality of any ransom payments; and maintaining clear communications with customers, consumers and other relevant stakeholders.

The only way to effectively prepare for such an event is to think and plan ahead. Conduct both technical and executive-level tabletop exercises involving all appropriate stakeholders to walk through these issues now and develop a comprehensive plan.

By doing so, companies will be much better prepared to understand how these workstreams will unfold in practice, tailored specifically to their own systems, products and other unique circumstances.

---

[1] U.S. Securities and Exchange Commission. “Compliance and Disclosure Interpretations: Exchange Act Form 8-K.” SEC.gov, https://www.sec.gov/rules-regulations/staff-guidance/compliance-disclosure-interpretations/exchange-act-form-8-k.

[2] *Id*. (citing Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release Nos. 33-11216; 34-97989 (July 26, 2023), 88 Fed. Reg. 51896, 51917 (Aug. 4, 2023)).

[3] *Id*. (citing Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release Nos. 33-11216; 34-97989 (July 26, 2023), 88 Fed. Reg. 51896, 51906 (Aug. 4, 2023)).

RELATED INDUSTRIES + PRACTICES

- Capital Markets
- Incidents + Investigations
- Privacy + Cyber
- Securities Investigations + Enforcement
- Securities Litigation