Privacy Alert
July 2024

SEC Issues Guidance on Material Cybersecurity Incidents

The Securities and Exchange Commission (SEC) has issued new guidance on disclosure obligations of material cybersecurity incidents. On June 24, the staff of the Division of Corporation Finance released five new Compliance & Disclosure Interpretations (CDIs) about disclosure obligations under Item 1.05 of Form 8-K. These supplement four previous CDIs addressing the effect of consultation with or national security findings by the attorney general. Below is a summary of the recent CDIs.

- **Resolution of a ransomware attack before the company makes a materiality determination does not absolve the company of its obligation to make a materiality determination:** The resolution or apparent resolution of the incident prior to the materiality determination does not necessarily indicate that the incident was not material, and the company must still make a determination. If a company experiences a cybersecurity incident involving a ransomware attack and, prior to any materiality determination by the registrant, the registrant pays the ransom and the threat actor ends their disruption of operations and returns any exfiltrated data, the registrant must still make a determination regarding the incident's materiality.
- **Even after a material cybersecurity event ends, it must still be disclosed:** A cybersecurity incident that a company determines to have had a material impact, or that is reasonably likely to result in a material impact, must disclose it on a Form 8-K within four business days after the company makes a materiality determination, even if the resolution or apparent resolution of the incident occurs prior to the filing of the Form 8-K.
- **Insurance coverage:** When determining whether a cybersecurity incident is material, the fact that a company received reimbursement for a ransomware payment under a cyber-insurance policy does not mean that the incident is not material. Companies must consider all relevant facts and circumstances, including both quantitative and qualitative factors such as the near-term and long-term effects on a company's operations, finances, brand perception and customer relationships, among other factors, when making a materiality determination.
- **Amount of ransomware payment:** The size of the ransomware payment, by itself, is not determinative of whether a cybersecurity incident is material. Instead, the size of the payment is only one factor relevant to a company's materiality determination.
- **Related immaterial cybersecurity events:** If a company experiences a series of cybersecurity incidents that, individually, are determined to be immaterial, the registrant should consider whether multiple incidents might be related and, if so, determine

Attorney Advertising

whether the cybersecurity incidents, when viewed collectively, are material. For this position, the CDIs highlight that Item 106(a) of Regulation S-K includes in the definition of a cybersecurity incident "a series of related unauthorized occurrences," which, according to the adopting release, can be a series of attacks from a single actor, or attacks from multiple actors exploiting the same vulnerability.

The SEC's guidance notes that in assessing the materiality of the incident, companies should, as noted in the adopting release for Item 1.05 of Form 8-K, determine "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," notwithstanding the fact that the incident may have already been resolved. If a timely disclosure would pose a substantial risk to national security or public safety, a process exists for requesting a delay in reporting.

The Director of the Division of Corporation Finance also issued a statement on June 24 relating to the selective disclosure of cybersecurity incidents. In this statement, the director emphasized that the new rules do not prohibit companies from discussing an incident beyond what was included in Item 1.05 of Form 8-K. Still, companies would need to ensure that any such additional information provided to third parties complied with Regulation FD, which prohibits selective disclosure of material nonpublic information to certain persons.

Key Takeaways. Publicly traded companies should take the following steps to better ensure compliance with SEC cybersecurity incident reporting obligations:

- Train key personnel to (1) identify and address cybersecurity incidents, (2) ensure that they have access to members of management who participate in making materiality and disclosure determinations, and (3) ensure compliance with Regulation FD with respect to information about the incident that is not included in any public disclosure.
- Follow clear, consistent and reliable practices for rigorous and fulsome materiality assessments of cybersecurity incidents, which should involve appropriate subject matter experts and legal specialists. Be sure to assess the information being provided to third parties to ensure compliance with Regulation FD.
- Document materiality assessment processes with guidance from legal counsel.
- When a cybersecurity incident is deemed material, ensure timely and complete disclosure under Item 1.05; if the company has not yet determined that an incident is material, carefully evaluate the risks and opportunities of disclosure under Item 8.01.

To read the full guidance on the SEC's website, click here and here.

Related Professionals

Harry Valetk . . . . . hvaletk@loeb.com
Giovanni Caruso. . . . . gcaruso@loeb.com