BDO BULLETIN

SEC STAFF RELEASES MORE INTERPRETIVE GUIDANCE ON CYBERSECURITY INCIDENT DISCLOSURE

JUNE 2024

SUMMARY

SEC registrants ("registrants") must disclose material cybersecurity incidents under Item 1.05 of Form 8-K ("Item 1.05") within four business days from the date they determine the incident is material.

The SEC staff released five new Compliance and Disclosure Interpretations (C&DIs) on cybersecurity incidents disclosure, focusing on the materiality assessment and disclosure requirements under various scenarios involving ransomware attacks. The new C&DIs clarify that:

- If a cybersecurity incident is resolved before the due date of Item 1.05, registrants must still:
  - Assess the materiality of the incident
  - Disclose the incident under Item 1.05 if the incident is material
- When assessing the materiality of an incident, registrants may not base their conclusion solely on the amount of net cash payments (e.g., ransomware payments less any related insurance proceeds)
- Multiple incidents may be individually immaterial, but require disclosure under Item 1.05 if they are related and collectively material

MATERIAL CYBERSECURITY INCIDENTS DISCLOSURE

The C&DIs address situations in which a cybersecurity incident has occurred, resulting in the exfiltration of a registrant's data or a disruption to the registrant's operations and the registrant makes a ransomware payment upon which the extracted data is returned or the disruption to its operations ceases. The C&DIs specifically address the following questions:

C&DI	GUIDANCE
If the ransomware payment occurs before the registrant makes a materiality determination, does the registrant need to assess whether the incident is material? (104B.05)	Yes. The registrant must assess the materiality of the incident, even though the incident is resolved (that is, the resolution of the incident does not alleviate the registrant's obligation to determine the materiality of the incident). If material, the registrant must report the incident under Item 1.05 within four business days from the date it determined the incident is material.
If the registrant determines the incident is material, but the ransomware payment is made before filing Item 1.05, does the registrant need to disclose the incident? (104B.06)	Yes. The registrant must report the incident under Item 1.05 within four business days from the date it determined the incident is material. The resolution of the incident does not exempt the registrant from disclosure under Item 1.05.
If under its insurance policy, the registrant is reimbursed for all (or most) of the ransomware payment made, is the incident immaterial? (104B.07)	Not necessarily. The registrant may not conclude the incident is immaterial based solely on the fact that all or a substantial portion of the ransomware payment was reimbursed under its insurance policy. When determining whether the incident is material, the registrant must consider all relevant facts and circumstances, including both quantitative and qualitative factors. For example, the registrant may consider an increase in the cost and availability of future insurance policies that cover cybersecurity incidents.
If the ransomware payment is a small dollar amount, is the incident immaterial? (104B.08)	Not necessarily. The registrant may not conclude the incident is immaterial based solely on the quantitative harm to the registrant (for example, the small amount paid). Qualitative factors, such as reputational harm, must also be considered.

Additionally, the definition of a cybersecurity incident includes "a series of related unauthorized occurrences" to reflect that cyberattacks sometimes compound over time, rather than at a point in time. As such, registrants that experience multiple cybersecurity incidents determined to be individually immaterial, may be required to disclose the incidents under Item 1.05 if the incidents are related and collectively material (104B.09). In the adopting release for the final rules, the SEC gave the following examples:

- The same malicious actor engages in small but continuous cyberattacks against the registrant and collectively, they are material
- A series of related attacks from multiple actors attack the same vulnerability and collectively, impede the registrant's business in a material way

Evaluating whether a series of related unauthorized occurrences are collectively material to the registrant may require the application of professional judgment, based on the facts and circumstances.

* * * * *

BDO Bulletin: **The SEC's New Cybersecurity Disclosure Rules are Here**

BDO Bulletin: **SEC Staff Releases New Interpretive Guidance on Cybersecurity Incident Disclosure**

BDO Bulletin: **SEC Staff Statement on Cybersecurity Incident Disclosure**

CONTACTS

TIMOTHY KVIZ
National Managing Principal, SEC Services
tkviz@bdo.com

PAULA HAMRIC
Professional Practice Principal, SEC Services
phamric@bdo.com