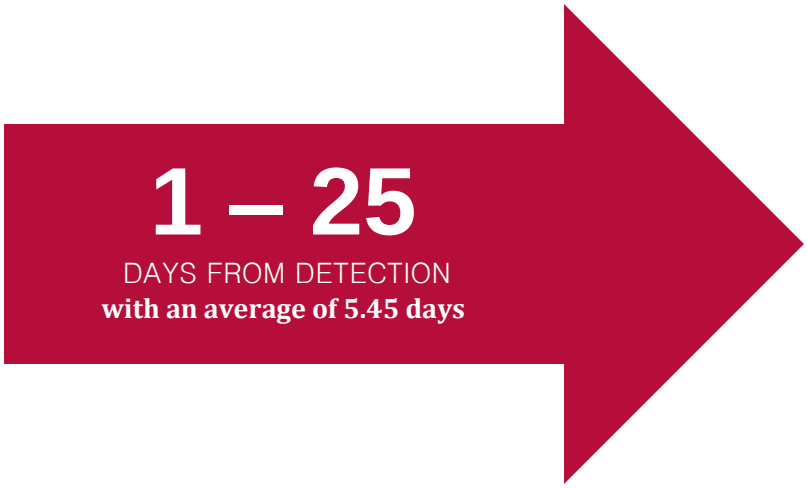
100 Days of Cybersecurity Incident Reporting on Form 8-K: Lessons Learned

March 28, 2024

On December 18, 2023, the Securities and Exchange Commission's (the "SEC") rule requiring disclosure of material cybersecurity incidents became effective. To date, 11 companies have reported a cybersecurity incident under the new Item 1.05 of Form 8-K ("Item 1.05").[1] After the first 100 days of mandatory cybersecurity incident reporting, we examine the early results of the SEC's new disclosure requirement.

Timing of Cyber 8-Ks



Item 1.05 requires an issuer to file a Form 8-K disclosing specified information about a cybersecurity incident within four business days of determining that the cybersecurity incident is material. This four-business-day deadline runs from the materiality determination, rather than the occurrence or detection of the incident, and the SEC has acknowledged that "[i]n the majority of cases, the registrant will likely be unable to determine materiality the same day the incident is discovered." In practice, however,

[1] One registrant, V.F. Corporation, reported a cybersecurity incident under Item 1.05 on December 15, 2023. Since Item 1.05 became effective, five registrants have filed Item 8.01 (Other Events) Form 8-Ks disclosing cybersecurity incidents. We do not address these Item 8.01 reports, and we, as a general matter, expect cybersecurity incidents to be disclosed under Item 1.05.

companies have disclosed incidents more quickly than the SEC may have anticipated. In the first 100 days, the average time from *detection* of a cybersecurity incident to the disclosure of the incident on a Form 8-K under Item 1.05 has been 5.45 business days. Eight companies (*i.e.*, over 70% of the sample) have filed Forms 8-K under Item 1.05 within four business days of *detecting* the cybersecurity incident.

While all disclosure decisions will necessarily be driven by the facts and circumstances surrounding the incident, including regulatory or contractual notification requirements, companies should take care not to rush disclosure in the "fog of war." In adopting Item 1.05, the SEC acknowledged that registrants will need to "develop information after discovery until it is sufficient to facilitate a materiality analysis." The Rule, therefore, allows companies to undertake a reasonable investigation and an informed and deliberative materiality analysis, provided companies do not "unreasonabl[y] delay" the required determination. In most instances, we believe companies are well-advised to exercise caution before rushing to disclose early in the course of an incident investigation. Still, sometimes the incident will have public ramifications which may merit very quick disclosure.

Substance of Cyber 8-Ks

Disclosure of Material Impacts

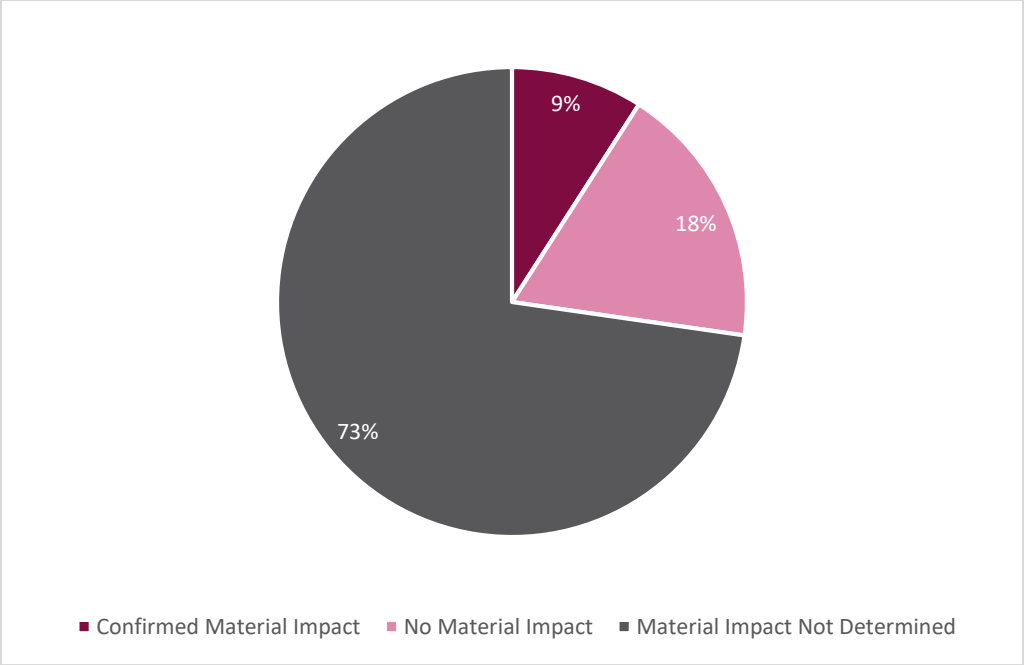
Of the 11 companies that have filed Forms 8-K to report a cybersecurity incident under Item 1.05, one identified a material operational disruption in its initial filing, and another identified a material impact on its results of operations in an amended filing made three weeks after the initial filing. The other nine companies did not expressly identify a material impact. They generally included an affirmative statement that the

incident had not materially impacted operations, and they typically stated that they had not determined the incident was reasonably likely to materially impact the Company's financial conditions or results of operations. The latter statement tracks Item 1.05's line-item requirement to disclose whether the incident materially impacts the company's financial condition and results of operations.

This trend has led to speculation that companies are voluntarily reporting immaterial cybersecurity incidents under Item 1.05 of Form 8-K or failing to adequately respond to Item 1.05's requirements. Alternatively, these nine companies may believe that the combined characteristics of the incident—such as operational disruption, data loss or scope and length of intrusion—comprise the material impacts, in that these or other factors considered together render the cybersecurity incident material, even where no one impact is considered independently material. It is also possible that the SEC's mandatory disclosure rule has caused a reassessment of when a cybersecurity incident could be considered material—especially incidents with possible qualitative material impact (*e.g.*, reputational or legal) but no quantitative material impact—potentially lowering the bar for disclosure.

Disclosure of Financial Impact

Material Impact on Financial Condition and Results of Operations



As noted above, one company disclosed that a cybersecurity incident was expected to materially impact the relevant quarter's results of operations. Two other companies

disclosed their belief that the relevant cybersecurity incident would not, or was not reasonably likely to, materially impact their financial condition or results of operations. The remaining eight companies disclosed that they had not, or had not yet, determined that the cybersecurity incident was reasonably likely to materially impact their financial condition or results of operations.

The SEC previously postulated that "most organizations' materiality analyses will include consideration of the financial impact of a cybersecurity incident, so information regarding the incident's impact on the registrant's financial condition and results of operations will likely have already been developed when Item 1.05 is triggered." However, this prediction has not been borne out during the first 100 days of mandatory disclosure. This may be due in part to the speed with which companies have disclosed cybersecurity incidents following detection. It also may reflect the difficulty of predicting financial impacts of cybersecurity incidents, the impacts of which are often more qualitative in nature.

Disclosure of Operational Disruptions

55%

OF ISSUERS HAVE DISCLOSED AN OPERATIONAL DISRUPTION

More than half of the companies that have reported a cybersecurity incident under Item 1.05 disclosed, either in their initial Form 8-K or an amendment, an operational disruption related to the cybersecurity incident. In contrast to financial or more qualitative (*e.g.*, reputational) impacts, operational disruptions may be more readily identifiable in the early stages of an incident, when disclosure decisions are typically being made. Indeed, the operational disruptions disclosed by five companies were caused, at least in part, by efforts to remediate or mitigate the incidents. Notably, however, only a single company disclosed that the operational disruption was material to its business operations.

Access to, or Loss of, Customer or Client Data

45%

OF ISSUERS HAVE SUFFERED LOSS OF DATA

Five companies have disclosed a cybersecurity incident that resulted in access to or exfiltration of data, such as client or customer data, or information contained within corporate email accounts. Three of these companies disclosed the nature of the exfiltrated data or the information targeted by the relevant threat actor in the initial Form 8-K, while two disclosed this information in a subsequent Form 8-K amendment.

Although the possibility of data loss may be known very early during the incident response, it may take a significant amount of time to identify all potential avenues of access or exfiltration, and to determine exactly what data was accessed or taken. The disclosure trend suggests that attacker access to potentially significant data, or a significant volume of data, are factors weighing in favor of disclosure, even if the nature of the data and whether it was, in fact, taken are the subject of ongoing investigation. This may be due, in part, to the risk that data exposure will trigger other notification requirements, such as notifications to customers, business partners or regulators, or pursuant to the Critical Infrastructure Act. Companies should take care when disclosing potential data loss early in an investigation, however, as the facts may continue to develop over an extended investigation, potentially triggering requirements to update or revise notices and disclosure related to the incident.

Identification of Threat Actors

36%

OF ISSUERS HAVE IDENTIFIED A THREAT ACTOR

Four of the cybersecurity incidents reported on Item 1.05 included identification—by name or nature—of the suspected threat actor. Three companies initially disclosed the potential involvement of a nation-state actor, two of which identified Midnight Blizzard/Cozy Bear. However, one company that initially attributed the incident to a nation-state later amended its 8-K to disclose that the threat actor was actually a cybercrime group. The remaining

company disclosed the potential involvement of cybercrime group, without identifying the suspected threat actor by name.

Item 1.05 calls for a description of the "nature" of the cybersecurity incident. This could be interpreted to include the nature of the threat actor where that is relevant to an understanding of the incident and its potential impacts. For instance, because nation-state actors may be very difficult to detect and fully remove from information systems, it is possible that the SEC would regard the involvement of these threat actors as relevant to an investor's understanding of the nature, scope and likely impacts of the incident. On the other hand, involvement of non-nation-state actors may also be indicative of the motives behind an incident, such as extortion or ransom payments. In either case, it is important to consider whether identification of the threat actor would impede the company's response or remediation of the incident. If so, that information may be omitted pursuant to Instruction 4 of Item 1.05.

Form 8-K Amendments

45%

OF ISSUERS HAVE FILED AN AMENDMENT

To the extent any required information is not determined or is unavailable at the time of filing a Form 8-K under Item 1.05, the company is required to file a Form 8-K amendment containing such information within four business days after the information is determined or becomes available.

Five companies have filed Form 8-K amendments. These amendments have disclosed remediation of the relevant cybersecurity incident, details regarding the impact of the incident (including reaffirmation of the material or immaterial nature of certain impacts), further actions taken by the threat actor and details regarding the nature of the incident. The relative frequency with which amendments have been filed underscores the difficulty inherent in cybersecurity incident disclosure: incidents and investigations evolve rapidly and unpredictably, leading to a need to update disclosure, particularly when disclosure is initially made in the early days of an investigation. Companies should ensure that their disclosure controls and procedures are attuned to

identify, escalate and assess significant new information during the course of an incident response.

SEC Comment Letter

The SEC's expectation for prompt amendments by reporting companies was confirmed just three weeks after the new rule took effect. On January 5, 2024, the Staff of the SEC (the "Staff") issued a comment letter to V.F. Corporation in respect of its Item 1.05 Form 8-K filed on December 15, 2023. The Staff cited V.F. Corporation's disclosure that "the full scope, nature and impact of the incident are not yet known" and that "[t]he Company has not yet determined whether the incident is reasonably likely to materially impact the Company's financial condition or results of operations." In its letter, the Staff requested that V.F. Corporation file an 8-K amendment, commenting that V.F. Corporation should "expand [its] discussion to describe the scope of [its] business operations impacted … describe the known material impact(s) the incident has had and the material impact(s) that are likely to continue" and "[i]n considering material impacts … describe all material impacts." The comment letter referred to vendor relationships and reputational harm as examples of potentially material impacts.

The Staff's comments serve as a reminder to companies to provide meaningful disclosure and actively monitor for potential updates to disclosure, especially when potentially significant information is unknown at the time of the initial filing. V.F. Corporation filed a Form 8-K amendment on January 18, 2024, disclosing additional information about the scope, nature and impact of the cybersecurity incident. Notably, however, the Form 8-K amendment did not disclose any additional material impacts of the cybersecurity incident.

Conclusion

After a quick start, with two incidents reported in the first week of effectiveness, a clear trend toward rapid disclosure has emerged, outpacing the kind of extended analysis of financial impacts that the SEC hypothesized most companies would undertake when determining materiality in the wake of a cybersecurity incident.

Overwhelmingly, companies that filed Forms 8-K under Item 1.05 during the first 100 days did not disclose a material impact on their financial results or their results of operations. Instead, companies have disclosed other characteristics of the cybersecurity incident that may have prompted disclosure, such as operational disruption, access to, or loss of, sensitive data and the involvement of specific threat actors.

Notwithstanding this trend towards speed, companies experiencing a cybersecurity incident would be well advised to exercise caution before disclosing too early in their

incident response. Though companies may not unreasonably delay, they can and should take the time needed to conduct a reasonable investigation of the facts to support an informed and deliberative materiality determination.

We will continue to monitor developments regarding material cybersecurity incidents reported on Form 8-K under Item 1.05 and will provide updates as they become available.

Our Cybersecurity Incident Disclosure Tracker can be found here.

To subscribe to our Data Blog, please click here.

* * *

Please do not hesitate to contact us with any questions.

Charu A. Chandrasekhar
Partner, New York
+1 212 909 6774
cchandra@debevoise.com

Erez Liebermann
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com

Benjamin R. Pedersen
Partner, New York
+1 212 909 6121
brpedersen@debevoise.com

Paul M. Rodel
Partner, New York
+1 212 909 6478
pmrodel@debevoise.com

Matt Kelly
Counsel, New York
+1 212 909 6990
makelly@debevoise.com

Anna Moody
Counsel, Washington, D.C.
+1 202 383 8017
amoody@debevoise.com

John Jacob
International Associate, New York
+1 212 909 6795
jjacob@debevoise.com

Kelly Donoghue
Associate, New York
+1 212 909 6145
kgdonogh@debevoise.com

Talia Lorch
Law Clerk, New York
+1 212 909 6707
tnlorch@debevoise.com