Blogs
May 22, 2024

As Allison Handy noted on our *Public Chatter* blog, Erik Gerding, the Director of the U.S. Securities and Exchange Commission (SEC) Division of Corporation Finance, issued a statement on May 21 clarifying public companies' obligations to disclose cybersecurity incidents under Item 1.05 of Form 8-K.

The statement looks like a response to the potential—and actual—"abundance of caution" filings in which public companies disclose that an incident occurred but do not announce whether the incident met the SEC's materiality threshold.

The message is clear: Voluntary disclosures are welcome under Item 8.01 (Other Events), but filing inconclusive reports under Item 1.05 (Material Cybersecurity Incidents) increases the signal-to-noise ratio such that investors

will not readily be able to understand the significance or impact of a cyber incident. As a result, companies that attempt both to avoid liability by making disclosures under Item 1.05 and to avoid concluding or acknowledging that they have suffered a material incident frustrate the purpose of the new disclosure rule, which is to give meaningful notice to investors about their investment decisions.

Companies that suffer a cyber incident have to determine whether or not the incident had a material impact on the company (even if that assessment changes with new information) and cannot hedge by filing under Item 1.05. Instead of making an inconclusive filing, Director Gerding advises that companies file under Item 8.01 to voluntarily disclose nonmaterial incidents and incidents for which materiality determinations have not been made and to update such filings under Item 1.05 if the company subsequently determines that the incident had a material impact. And if an incident is sufficiently severe that the victim company can conclude it will have a material impact, even if the specific impact or its scope cannot yet be determined, the company should file under Item 1.05 and update that disclosure once new information and analysis are available.

Finally, Director Gerding reiterated that materiality assessments should be holistic and should take into account qualitative as well as quantitative factors. Notices should give investors enough information for them to understand relevant facts regarding the nature, scope, and timing of the incident, as well as the incident's impact or reasonably likely impact.

More information about making materiality determinations and updating incident response plans to incorporate compliance with the SEC disclosure rules are available on the *Perkins on Privacy* blog.

Authors

David Aaron

Senior Counsel
DAaron@perkinscoie.com

Explore more in

Privacy & Security
Blog series

Perkins on Privacy

Perkins on Privacy keeps you informed about the latest developments in privacy and data security law. Our insights are provided by Perkins Coie's Privacy & Security practice, recognized by Chambers as a leading firm in the field. Subscribe ?

View the blog