JENNER & BLOCK

The SEC's Approach to Cybersecurity Disclosure Decisions

Client Alerts

June 26, 2024
By: Shoba Pillay, Charles D. Riely, H. Kurt von Moltke

The SEC's Director of Corporation Finance, Erik Gerding, recently issued two statements regarding a public company's disclosure obligations in response to a cybersecurity incident. These remarks follow the adoption of the SEC's new cybersecurity requirements for public companies last year, as well as a series of SEC cybersecurity enforcement actions, including *SEC v. SolarWinds et al.*, the developments of which we covered here and here. This client alert analyzes the key points of Mr. Gerding's statements in light of the SEC's cybersecurity enforcement landscape and provides takeaways for public companies.

Mr. Gerding's Statements Regarding a Public Company's Cybersecurity Disclosure Obligations in Response to a Cybersecurity Incident

The new cybersecurity rules require public companies to disclose "material" cybersecurity incidents under Item 1.05 of the Current Report on Form 8-K.[1] Following the adoption of the rules, some public companies who experienced cybersecurity incidents opted to disclose the incident pursuant to Item 1.05 of Form 8-K, presumably out of the abundance of caution, despite determining that at the time of the filing, the incident had not had a "material impact on the Company's operations," and that the "Company had not yet determined whether the incident is reasonably likely to materially impact the Company's financial condition or results of operations."[2]

On May 21, 2024, Mr. Gerding issued a statement discussing voluntary filings pursuant to Item 1.05 of Form 8-K, in which a public company either had not yet made a materiality determination, or determined that the incident was not material.[3] In these situations, Mr. Gerding stated that the SEC's Division of Corporation Finance "encourages a company to disclose that cybersecurity incident under a different item of Form 8-K (for example, Item 8.01)."[4] Item 8.01 (Other Events) of Form 8-K is an optional item that allows a company to disclose any events, with respect to which information is not otherwise called for by the other items of Form 8-K, that the company deems of importance to security holders. The company may also, at its option, file a report under Item 8.01 of Form 8-K disclosing the nonpublic information required to be disclosed by Regulation FD.[5] Mr.

Gerding explained that disclosing immaterial incidents under Item 1.05 would create investor confusion, noting that:

"Given the prevalence of cybersecurity incidents, this distinction between a Form 8-K filed under Item 1.05 for a cybersecurity incident determined by a company to be material and a Form 8-K voluntarily filed under Item 8.01 for other cybersecurity incidents will allow investors to more easily distinguish between the two and make better investment and voting decisions with respect to material cybersecurity incidents. By contrast, if all cybersecurity incidents are disclosed under Item 1.05, then there is a risk that investors will misperceive immaterial cybersecurity incidents as material, and vice versa."[6]

On June 20, 2024, Mr. Gerding issued a second statement to dispel "assertions that [the new cybersecurity rules] may preclude a company from sharing additional information about a material cybersecurity incident with others, including their commercial counterparties."[7] In his June statement, Mr. Gerding stated that "[n]othing in Item 1.05 prohibits a company from privately discussing a material cybersecurity incident with other parties or from providing information about the incident to such parties beyond what was included in an Item 1.05 Form 8-K."[8] While Mr. Gerding noted that public companies would still need to comply with the selective disclosure requirements of Regulation FD, he noted that there are several well-established ways in which companies can share information about an incident with third parties without increasing its exposure under Regulation FD.[9]

The SEC's Evolving Enforcement Landscape Regarding Cybersecurity

Mr. Gerding's statements come at a time when the SEC's Enforcement Division has significantly ramped up its scrutiny of how public companies address cybersecurity incidents. The SEC's disclosure enforcement cases include instances in which:

- A public company's technology and customer services personnel failed to immediately escalate information about the scope of a cybersecurity incident to those making disclosure decisions; [10]

- A public company investigated the incident, disclosed the incident to affected users whose data had been accessed, but decided not to disclose the incident to investors. In later disclosing the incident to investors, the company stated that a hacker had obtained a "subset of data" without disclosing that the data had been "sensitive";[11] and

- A public company disclosed an incident, noted that it was "still investigating whether and to what extent the vulnerability… was successfully exploited," but did not also admit that the vulnerability had already been exploited in the past.[12]

These cases signal that the SEC has high expectations for public companies in their ability to analyze, escalate, remediate, and make difficult disclosure decisions in the heat of the moment of a cybersecurity incident. Indeed, the SEC's current stance appears to be a presumption of disclosure across its enforcement program, regardless of whether the entity is still investigating the cybersecurity incident or facts regarding the incident are unclear or unknown.[13]

At the same time, materiality—which affects both the timing and substance of the disclosure for purposes of Item 1.05 of Form 8-K—continues to be an unsettled topic in cybersecurity. The SEC's cybersecurity enforcement cases have not emphasized classic, quantitative markers of materiality, such as a stock price decline or loss of revenue or customers in response to information about a cybersecurity incident. Rather, SEC enforcement actions appear to focus either on qualitative factors, including loss of reputation or the issuer's own risk factors discussing cybersecurity as an apparent admission of materiality. Accordingly, public companies are endeavoring to define materiality for cybersecurity incidents in a way that is tailored to their business, but without comfort that the SEC's Enforcement Division will necessarily agree with their analysis in the wake of a breach.

Given the uncertainties in cybersecurity disclosure, Mr. Gerding's statements that public companies should distinguish material from immaterial cybersecurity incidents in their disclosures, as well as walk the fine line of discussing an incident with third parties, may be difficult to apply in practice. It is not unsurprising that some public companies have elected to disclose a seemingly immaterial cybersecurity incident pursuant to Item 1.05 of Form 8-K, at least to avoid later criticism that they downplayed an incident that later turned out to be more serious.

In addition, companies face challenges in making disclosure decisions regarding their diverse constituents—e.g., their customers, clients, and contractual counterparties. Indeed, a key risk factor driving data breach litigation is when a company issues inconsistent statements to various third parties, revealing a lack of full transparency to all affected parties. That risk is exacerbated if the company makes further disclosures revealing inaccuracies in earlier disclosures due to information that is newly discovered in the course of its investigation. As threat actors and threat vectors become more sophisticated, companies face more complicated investigations, making the disclosure process daunting. Ultimately, while the SEC is pushing companies to make disclosures of cyber incidents on an accelerated basis, such early disclosure can hamper remediation measures being taken to eliminate or reduce the effects of the cyber incident, and can also potentially trigger a chain reaction of disclosures by counterparties that may result in an increase in the leverage of threat actors.

Key Takeaways

- An SEC enforcement action is a heightened risk for public companies following a major cybersecurity incident. The SEC's recent enforcement actions set forth high expectations for public companies and suggest that the SEC will not hesitate to use hindsight to second guess a

company's disclosure decisions and policies and procedures, in the event of a major cybersecurity incident.

- The SEC expects public companies to have well-defined and functioning disclosure practices and committees to ensure that important information is presented to the proper decision-makers, in order to make timely materiality determinations.

- The SEC will not allow public companies to use early generic disclosure of cyber incidents to avoid their responsibility to provide accurate and timely disclosure of cyber incidents that are later determined to be material or reasonably likely to become material.

Ultimately, public companies face considerable challenges in making appropriate disclosure decisions in an aggressive SEC enforcement environment while simultaneously dealing with a cybersecurity incident. Companies should ensure that they are prepared—from an incident response and disclosure policy perspective—before a major cybersecurity incident, and consult with counsel if faced with difficult disclosure decisions in the event of a breach.

Footnotes

[1] Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure, SEC Release Nos. 33-11216; 34-97989 (July 26, 2023), available at https://www.sec.gov/files/rules/final/2023/33-11216.pdf.

[2] Microsoft Corp., Current Report (Form 8-K) (Jan. 17, 2024).

[3] Statement of Director, Division of Corporation Finance, Erik Gerding, *Disclosure of Cybersecurity Incidents Determined to Be Material and Other Cybersecurity Incidents [*]* (May 21, 2024), available at https://www.sec.gov/news/statement/gerding-cybersecurity-incidents-05212024.

[4] *Id.*

[5] Item 8.01 (Other Events) of Current Report (Form 8-K).

[6] *Disclosure of Cybersecurity Incidents*, supra note 3.

[7] Statement of Director, Division of Corporation Finance, Erik Gerding, *Selective Disclosure of Information Regarding Cybersecurity Incidents* (June 20, 2024), available at https://www.sec.gov/news/statement/gerding-cybersecurity-incidents-06202024.

[8] *Id.*

[9] *Id.*

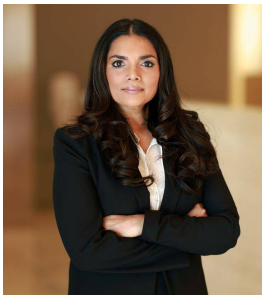
[10] SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors (Mar. 9, 2023), available at https://www.sec.gov/news/press-release/2023-48.

[11] SEC Charges Pearson plc for Misleading Investors About Cyber Breach (Aug. 16, 2021), available at https://www.sec.gov/news/press-release/2021-154.

[12] Amended Complaint ¶ 313, *SEC v. SolarWinds & Brown*, No. 1:23-cv-09518 (S.D.N.Y. Feb. 16, 2024), ECF No. 85.

[13] For instance, the SEC recently imposed a $10M penalty on a national securities exchange and its affiliates for running afoul of immediate reporting requirements of a breach even though the exchange determined within its four-day investigation that a cybersecurity incident had de minimis impact. SEC Charges Intercontinental Exchange and Nine Affiliates Including the New York Stock Exchange with Failing to Inform the Commission of a Cyber Intrusion (May 22, 2024), available at https://www.sec.gov/enforce/ap-summary/34-100206-s. Similarly, the recently adopted amendments to Regulation S-P require covered entities to notify any individuals reasonably affected by an incident even they cannot identify which specific individuals' sensitive customer information has been accessed or used without authorization. Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, 17 CFR §§ 240; 248; 270; 275 (2024).

Related Attorneys



Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605

Charles D. Riely
Partner
criely@jenner.com
+1 212 891 1686

H. Kurt von Moltke
Partner
kvonmoltke@jenner.com
+1 312 840 7499

Related Capabilities

Data Privacy and Cybersecurity

Public Company Advisory Group

Stay Informed →