Westlaw Today
powered by Reuters

Cybersecurity breaches: disclosure considerations amid increasing SEC scrutiny

By Brian R. Boch, Esq., Charles D. Riely, Esq., and William R. Erlain, Esq., Jenner & Block LLP

OCTOBER 15, 2021

Recent cybersecurity events have tested the cybersecurity defenses of many of America's largest public companies and given rise to private class actions and insider trading cases. At the same time, the U.S. Securities and Exchange Commission (the "SEC") has ramped up its enforcement against misleading cybersecurity disclosures and announced plans to consider adopting new disclosure obligations. Thus, companies may find their ability to respond to a cybersecurity event in real time tested on multiple fronts.

The best approach to ensure that a company is prepared for these tests and can navigate the potential pitfalls is advance preparation and planning. The reality is that when a cybersecurity breach occurs, it can present difficult and time-sensitive disclosure questions under the federal securities laws.

Management will need to dissect and analyze any cybersecurity breach that is capable of significantly impacting the company now or in the future.

This article highlights key factors to consider in determining whether and how a public company should disclose a cybersecurity breach in light of recent SEC guidance, enforcement actions and investigations, and private securities actions.[1] It also discusses recent events that demonstrate the SEC's Division of Enforcement is taking a close look at these issues.

Ultimately, a public company that has suffered a data breach has to evaluate the potential risk to its business, operations and financial performance and condition, the potential impact on its customers, vendors, employees and other constituencies, and the potential likelihood of regulatory scrutiny.

Disclosure obligations and SEC guidance

A key overarching principle of a company's periodic SEC reporting requirements is materiality. While Regulation S-K and SEC forms such as Forms 10-K and 10-Q mandate a number of specific line item disclosure requirements, the regulatory regime as a whole reflects the SEC's "long-standing commitment to a principles-based, registrant-specific approach to disclosure."[2]

The SEC has alluded to the fact that cybersecurity issues are often too dependent on facts and circumstances to prescribe specific disclosure obligations.[3] Consequently, public companies must disclose data breaches in their SEC reports to the extent they are material in ways important to a reasonable investor.

What to disclose

Over the last decade the SEC has released guidance that outlines how public companies should assess materiality with respect to cybersecurity breaches. The SEC emphasizes that companies should consider "the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact of the incident on the company's operations."

In this context, materiality depends on the "nature, extent, and potential magnitude" of the breach, including the possible harm to the company's "reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities."

In other words, management will need to dissect and analyze any cybersecurity breach that is capable of significantly impacting the company now or in the future. That said, a company is not required to disclose every single cybersecurity issue that is uncovered, but it will need to report the "risks and incidents that are material to investors."

SEC guidance also discusses the many ways in which a material cybersecurity breach may need to be disclosed in SEC filings. In the first instance, a company should consider updating each element of disclosure in a periodic report to which a cybersecurity breach is material. For example, if the details of a material trade secret are stolen through a data breach, the company may need to:

(1) update its MD&A disclosure to discuss any material effect on its current or future results of operations and financial condition,

(2) update its Legal Proceedings disclosure to describe any resulting material legal proceeding involving the company or its subsidiaries, and even

(3) update its Description of Business disclosure to reflect any material change in its competitive position.

A company must also assess whether any additional information needs to be disclosed if doing so is "necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading."

Moreover, the SEC emphasizes that Risk Factor disclosures should also be carefully reviewed and updated in light of a material cybersecurity breach. At a minimum, this would include updating any risk factors that describe a cybersecurity breach as a mere possibility if a material breach has in fact already occurred.

In this instance, SEC guidance counsels that a company "may need to discuss the occurrence of that cybersecurity incident and its consequences as part of a broader discussion of the types of potential cybersecurity incidents that pose particular risks to the company's business and operations."

When to disclose

SEC guidance also counsels on the timing of disclosures following a material cybersecurity breach. While a company may need some time to ascertain the relevant facts to be disclosed, a company cannot simply rely on the fact that its investigation is ongoing as a basis for omitting any required disclosure of a material breach in any of its periodic SEC reports, including its Form 10-K and 10-Q filings.

The SEC has brought a number of enforcement actions relating to various companies' disclosure of cybersecurity breaches.

That said, the guidance acknowledges that "some material facts may not be available at the time of the initial disclosure," that a company "may require time to discern the implications of a cybersecurity incident," and that "ongoing investigation of a cybersecurity incident may affect the scope of disclosure regarding the incident."

However, the time to report is not indefinite, and the SEC guidance specifically states that "an ongoing internal or external investigation — which often can be lengthy — would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident."

In this regard, a public company should be mindful of its quarterly deadlines for filing periodic reports. A company's management team, particularly those responsible for disclosure determinations, should be sufficiently informed about all significant developments related to the investigation of a potentially material cybersecurity breach so that an informed decision can be made about any potential disclosure implications prior to filing.

Furthermore, a company engaging in a public securities offering or other capital markets transaction (including stock repurchases) should be mindful of the need to ensure that all material non-public information is appropriately disclosed at the time of such transactions.

Potential future rule changes

The SEC indicated in a recent regulatory agenda that the SEC's Division of Corporation Finance is "considering recommending that the [SEC] propose rule amendments to enhance issuer disclosures regarding cybersecurity risk governance."[4]

It is unclear at this time what specific changes will be proposed, but SEC Chair Gary Gensler has made clear his intent to bolster public disclosures in the interest of investor protection.[5]

Risk of SEC enforcement action

The stakes in getting disclosures relating to cybersecurity breaches and risks is high because it is clear that the SEC is closing scrutinizing company disclosures in this area. The SEC has brought a number of enforcement actions relating to various companies' disclosure of cybersecurity breaches. These actions demonstrate that the SEC takes seriously cybersecurity breach disclosure deficiencies.

In its first major case in this area, the SEC charged Altaba, formerly known as Yahoo!, in 2018 for failing to disclose a breach of user data for more than 500 million accounts.[6] Yahoo! allegedly failed to investigate both the breach itself and whether the breach needed to be disclosed, and ultimately did not disclose the breach for two years.

The SEC alleged that Yahoo!'s financial statements during those two years were materially misleading because they failed to disclose the breach. At the time of this SEC action, the Co-Director of the SEC's Division of Enforcement underscored that while the SEC does not "second-guess good faith exercises of judgment about cyber-incident disclosure," the Yahoo! breach and lack of response were "so lacking that an enforcement action [was] warranted."

In addition, the SEC's order noted that Yahoo! did not share the breach with its auditors, and failed to maintain proper internal controls to ensure that "cyber breaches, or the risk of such breaches, were properly and timely assessed for potential disclosure."

There have been more recent indications that the SEC is continuing to focus on this area and there are signs that its expectations for public companies are increasing. In mid-June 2021, the SEC settled charges against a real estate settlement company "for disclosure controls and procedures violations related to a cybersecurity vulnerability that exposed sensitive customer information."[7]

That is, the SEC brought a case related to perceived vulnerability and not an actual breach. As detailed in the SEC's order, the vulnerability at issue involved the potential exposure of customer information such as financial information and social security numbers.

The SEC alleged that, when questioned about the potential vulnerability by a cybersecurity journalist, the real estate settlement company issued a statement approved by senior management that left out key facts relating to the company's response to the breach. The crux of the SEC's case was that the company failed to have adequate policies and procedures to guarantee that the people making the disclosure had addressed to the relevant facts.

Then in mid-August 2021, the SEC settled charges against a foreign educational publishing and services company relating to the company's handling of a 2019 cyber intrusion.[8] In the wake of discovering that a third party had improperly accessed and downloaded millions of rows of data containing login and personal information about students and school personnel, the company did not publicly disclose the incident nor update its risk factor discussing the potential for a data privacy incident to occur.

When the company later publicly disclosed the incident in response to an impending news article, the media statement failed to disclose that data was downloaded — rather than simply viewed — and downplayed the scope of information that was taken.

Accordingly, the SEC concluded that the unchanged risk factor "implied that no 'major data privacy or confidentiality breach' had occurred" and the media statement failed to apprise impacted parties about the circumstances surrounding the breach.

There is, of course, no set playbook that will dictate exactly how to respond to each individual cybersecurity event or cybersecurity risk.

Additionally, in an unusual move, the SEC staff acknowledged in June 2021 that it is "conducting an investigation regarding a cyberattack involving the compromise of software made by the SolarWinds Corp., which was widely publicized in December 2020 (the "SolarWinds Compromise").[9]

The SEC staff has stated that it sent a request to companies it believes were impacted by the SolarWinds Compromise. Although the requests offer relief in certain circumstances, companies are actively wrestling with the narrow scope of that relief. Regardless of how this initiative turns out, it serves as more evidence that the SEC is focused on ensuring companies make adequate and timely disclosures about cybersecurity events.

There is, of course, no set playbook that will dictate exactly how to respond to each individual cybersecurity event or cybersecurity risk. But it is essential that companies consider the very real possibility that the disclosure decisions will be second-guessed when crafting their response.

If a request from the SEC's Division of Enforcement is ultimately received, a company would want to be able to show that its public statements were reasonable under the circumstances, that no material risks were omitted, and that there were no misstatements.

Risk of insider trading

A cybersecurity breach can also create significant insider trading risk for company insiders. For example, after a 2017 cybersecurity breach at Equifax that impacted over 148 million U.S. consumers, two Equifax employees sold some of their Equifax stock holdings prior to the public disclosure of the breach.

In separate actions, both the Department of Justice and the SEC pursued insider trading claims against the Equifax employees.[10] The government alleged that these Equifax employees had misused confidential information they obtained in the course of their employment to sell stock before Equifax disclosed the breach.

Risk of private securities actions

In addition to garnering regulatory scrutiny, cybersecurity breaches have resulted at times in private securities lawsuits. For example, the Equifax cybersecurity breach led to a securities class action and derivative action, which it ultimately settled for $149 million and $32.5 million, respectively.

In a shareholder derivative suit filed in September 2019, plaintiff stockholders accused FedEx of making materially misleading statements in connection with a cyberattack.11 As these cases indicate, the failure to disclose cybersecurity breaches can potentially lead to allegations of disclosure deficiencies and the resulting risk of significant liability in private causes of action.

Conclusion

In the end, a company may not be able to protect itself from every potential cybersecurity breach. However, a company's management team should be prepared for the possibility that a cybersecurity breach may occur, and accordingly would be wise to maintain robust internal controls and make a habit of keeping key disclosure decision-makers apprised of any evolving situation so that decisions about appropriate disclosure can be made on an informed basis.

Notes

[1] While this article focuses on disclosure obligations under SEC rules, companies should also be mindful of state laws that require notification to consumers and/or state attorneys general after significant data breaches.

[2] *Modernization of Regulation S-K Items 101, 103, and 105*, Release Nos. 33–10825; 34–89670 at 63727 (Oct. 8, 2020), https://bit.ly/3FBJfEd

[3] *See id*. at 63744 (declining to add a cybersecurity-specific risk factor disclosure).

[4] Office of Information and Regulatory Affairs, Office of Management and Budget, "Cybersecurity Risk Governance," https://bit.ly/3mMlKje; *see also* SEC, SEC Announces Annual Regulatory Agenda (June 11, 2021), https://bit.ly/30gWydf

[5] See, e.g., Gary Gensler, Prepared Remarks at London City Week (June 23, 2021), https://bit.ly/3DwTTdS

[6] SEC, Altaba, Formerly Known as Yahoo!, Charged with Failing to Disclose Massive Cybersecurity Breach; Agrees to Pay $35 Million (Apr. 24, 2018), https://bit.ly/3oRPrlD

[7] SEC, SEC Charges Issuer with Cybersecurity Disclosure Controls Failures (June 15, 2021), https://bit.ly/3iPRYJg

[8] SEC, SEC Charges Pearson plc for Misleading Investors About Cyber Breach (Aug. 16, 2021), https://bit.ly/307wGAk

[9] SEC, In the Matter of Certain Cybersecurity-Related Events (HO-14225) FAQs, https://bit.ly/3AwPOnS

[10] *See* Complaint, *SEC v. Bonthu*, No. 18-cv-3114 (N.D. Ga. filed June 28, 2018); Complaint, *SEC v. Ying*, No. 18-cv-1069 (N.D. Ga. filed Mar. 14, 2018).

[11] *See* Complaint, *Flaker v. Barksdale*, No. 19-cv-1747 (D. Del. filed Sept. 17, 2019).

About the authors



Brian R. Boch (L), a partner in **Jenner & Block**'s corporate department, focuses his practice on capital markets transactions, mergers and acquisitions, securities compliance and corporate governance. Based in the firm's Chicago office, he may be reached at bboch@jenner.com. **Charles D. Riely** (C) is a New York-based partner in the firm's investigations, compliance and defense practice and a former assistant regional director for the Division of Enforcement for the U.S. Securities and Exchange Commission. He may be reached at criely@jenner.com. **William R. Erlain** (R) is an associate in the firm's corporate department, based in Chicago. He may be reached at werlain@jenner.com. The authors thank a former associate of the firm, Logan Gowdey, for his assistance in this article.

This article was first published on Westlaw Today on October 15, 2021.