JENNER & BLOCK

Client Alert: SEC's Approach to Enforcement After Cyber Incidents: Key Takeaways for Public Companies from a Recent Speech

Publications

July 6, 2023
By: Shoba Pillay, Charles D. Riely

Last month, Gurbir Grewal, the Director of the SEC's Division of Enforcement, spoke at the Financial Times Cyber Resilience Summit. During the remarks, he outlined the importance of cybersecurity and signaled that the SEC is taking an aggressive stance against public companies that fail to take the right steps after experiencing a cyber incident.

Grewal's comments come amid proposed changes to SEC rules that would require public companies to disclose "a material cybersecurity incident within four business days" after learning of "a material cybersecurity incident."[1] These requirements accompany other anticipated changes to SEC rules designed to enhance disclosures regarding cybersecurity risk management and incident reporting by financial institutions. While these changes could usher in a set of new requirements, Grewal's speech made clear that the SEC will continue to pursue enforcement under current law. This article discusses the key takeaways for public companies.

SEC Enforcement Action Following a Cyber Incident Is a Heightened Risk

Grewal acknowledged that, whatever its precautions, a company will experience cyber incidents. As Grewal noted at the outset of his remarks, "cyber *resilience* is a concept that recognizes that breaches and cyber incidents *are* likely going to happen, and that firms must be prepared to respond appropriately when they do. In other words, it's not a matter of if, but when."[2]

Despite the inevitability of these incidents, Grewal exhibited little sympathy for companies that mishandle reporting obligations when faced with the crisis of responding to a cyber incident. He stated that he had "zero tolerance for gamesmanship around the disclosure decision."[3] He advised executives to disclose concerns about a data breach to the SEC "sooner rather than later"—even if you only "think you might" have a material event to disclose—and regardless of whether your company has finished its internal investigation into the incident.[4]

Grewal emphasized that, when there are cyberattacks on publicly traded companies, the SEC considers the investing public to be potential victims of those incidents. Decisions made within companies regarding whether to disclose a cyber incident can affect the company's customers, whose personal identifying information may have been compromised, or the company's investors, who need to be apprised of material information. And when delayed disclosure leads to increased risk to the public, the SEC may come knocking.

Grewal's rhetoric is consistent with the SEC's increasingly aggressive approach to enforcement actions involving cyber incidents. For instance, earlier this year, the SEC settled charges against Blackbaud, Inc., a data management company, in connection with misleading investors about the scope of a ransomware attack.[5] Over the course of three months, the company initially indicated that the attack had not involved certain information about donors, then learned through its technology and customer personnel that such exfiltration had occurred, and ultimately disclosed the full scope of the attack.[6] The SEC required the company to pay $3 million in penalties despite the relatively short timeframe in which the company made its complete disclosures regarding the attack and the absence of a finding that the company acted intentionally.[7]

Today, the SEC appears even more willing to expand the scope of liability involving cybersecurity incidents. For instance, in the case of SolarWinds Corporation—whose ubiquitous network management software was found to be compromised in 2020—the SEC has taken the unprecedented step of signaling enforcement actions against both the company and its senior executives. The SEC recently issued formal notifications, known as Wells Notices, to the CFO and CISO of SolarWinds, alerting them of potential civil enforcement actions stemming from the SEC's investigation into the cyberattack.[8]

The SolarWinds investigation will be one to watch to gain more insight into the SEC's enforcement trends, but as of now, the SEC appears ready to hold executives within public companies accountable for data breaches and related disclosures and controls issues. Executives managing cyber risk will want to tread with caution and review their insurance policies to ensure their coverage in the event of fallout from a cyber incident.

Companies Need to Enhance Policies Designed to Prevent Cyber Incidents and Err on the Side of Careful Disclosure When They Occur

Grewal urged companies to update their cybersecurity policies to keep up with evolving threats, to ensure that the right information is passed up the chain to executives making disclosure decisions, and to disclose major cybersecurity incidents immediately after they happen. As Grewal noted, the SEC has previously sued companies for having deficient disclosure controls and procedures relating to cyber incidents.

In one example Grewal cited, the SEC charged First American Financial Corporation, a title insurance company, with disclosure controls and procedures violations related to a cybersecurity vulnerability

that exposed sensitive customer information.[9] There, company IT personnel identified the vulnerability but failed both to fix it and to report it to senior executives. Months passed, and First American disclosed the vulnerability only after a reporter brought it to the company's attention.

In another example, the SEC charged Pearson, an educational publishing company, with misleading investors about a cyber intrusion involving the theft of personal data regarding student records.[10] In public statements, Pearson had referred to a data-privacy incident as a hypothetical risk (even though the breach had already occurred), disclosed the incident only after being contacted by the media, and later understated the severity of the incident. Although the SEC's settlement reflected negligence-based charges against the company and acknowledged that the right information had not passed up the chain to those making disclosure decisions, Grewal referred to this case as an example of gamesmanship around disclosure decisions and warned that penalties in future cases would be higher.[11]

Grewal's speech signals that the Enforcement Division is approaching public companies' responses to cyber incidents with increasing skepticism and will not hesitate to bring enforcement actions. As companies face increasingly sophisticated cybersecurity threats, companies should ensure that their cybersecurity policies are continuously updated, and that their disclosure decisions about cybersecurity incidents reflect careful, well-substantiated, and documented judgment.

Conclusion

Responding to news of a cyber vulnerability or a data breach is difficult enough. The risk of an SEC enforcement action against your company or officers only adds to the problems. Companies should consult with counsel who are familiar with both cyber risk management and SEC enforcement to ensure that they are prepared for cyber incidents and are able to respond appropriately when one occurs.

Jenner & Block will continue to monitor the regulatory landscape surrounding the SEC and cybersecurity.

Footnotes

[1] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16,590, 16,595 (proposed Mar. 23, 2022) (to be codified at 17 C.F.R. § 249.308), https://www.federalregister.gov/documents/2022/03/23/2022-05480/cybersecurity-risk-management-strategy-governance-and-incident-disclosure; *see also* Press Release, U.S. Sec. & Exch. Comm'n, SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (Mar. 9, 2022), https://www.sec.gov/news/press-release/2022-39.

[2] Gurbir S. Grewal, Director, U.S. Sec. & Exch. Comm'n Div. of Enf't, Remarks at Financial Times Cyber Resilience Summit (June 22, 2023), https://www.sec.gov/news/speech/grewal-financial-times-cyber-resilience-summit-06222023.

[3] *Id.*

[4] *Id.*

[5] *See* Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors (Mar. 9, 2023), https://www.sec.gov/news/press-release/2023-48.

[6] *See* Blackbaud, Inc., Securities Act Release No. 11,165, Exchange Act Release No. 97,098 (Mar. 9, 2023), https://www.sec.gov/litigation/complaints/2023/comp-pr2023-48.pdf.

[7] *See id.* at 6.

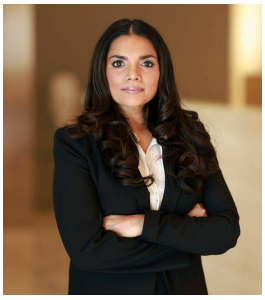
[8] SolarWinds Corp., Current Report (Form 8-K) (June 23, 2023), https://d18rn0p25nwr6d.cloudfront.net/CIK-0001739942/02aed9ff-6065-4158-8efd-6b5e31f7eb89.pdf.

[9] *See* Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges Issuer With Cybersecurity Disclosure Controls Failures (June 15, 2021), https://www.sec.gov/news/press-release/2021-102.

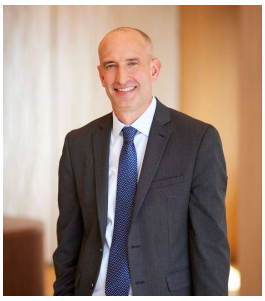
[10] *See* Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges Pearson plc for Misleading Investors About Cyber Breach (Aug. 21, 2021), https://www.sec.gov/news/press-release/2021-154.

[11] Grewal, *supra* note 2.

Related Attorneys



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



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

Related Capabilities

Data Privacy and Cybersecurity

Investigations, Compliance, and Defense

Stay Informed →