BCLP. Client Intelligent

BCLPSecCorpGov.com

THE SEC IS WATCHING: FOUR COMPANIES CHARGED FOR MISLEADING CYBER DISCLOSURES

PRIVACY SPEAKS SERIES

Nov 06, 2024

On October 22, 2024, the U.S. Securities and Exchange Commission (SEC) charged four publicly traded technology companies with making materially misleading disclosures regarding cybersecurity risks and incidents (see SEC press release), ushering in a new era of risk for companies that do not take note of these enforcement actions and react accordingly.

As a reminder, the expanded cyber disclosure rules came into effect at the end of 2023 and require companies to disclose in Item 1.05 of Form 8-K any cybersecurity incident they determine to be material and to describe the material aspects of the incident's nature, scope, and timing, as well as its material impact or reasonably likely material impact on the company. This disclosure must be made within four business days after a company determines that a cybersecurity incident is material. Companies must also make broader disclosures in their annual 10-K filings and provide descriptions of their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company.

The SEC's latest enforcement actions involve the SolarWinds cyberattack, which involved state-sponsored hackers inserting malware into SolarWinds' Orion software updates, allowing attackers to access the networks of numerous SolarWinds customers, including several U.S. government agencies and private companies. As a result, many companies were impacted and required to disclose the incident as material in their public disclosures and/or otherwise reference it as part of their broader cybersecurity disclosures.

ALLEGATIONS

The SEC's investigation alleged that the four companies downplayed the severity of the SolarWinds-related intrusions in their public disclosures in a number of ways, including by:

- Describing the cybersecurity risks as a result of and after the SolarWinds incident as hypothetical.
- Minimizing the impact by stating that only a limited number of email messages were accessed, while attackers had actually accessed a significant number of files in their cloud sharing environment.
- Providing generic descriptions of cyber risks without disclosing the specific intrusion the company had experienced.
- Failing to disclose the nature and extent of the data exfiltrated by the attackers, including encrypted credentials.

The SEC also alleged that, in some cases, these materially misleading disclosures resulted in part from deficient disclosure controls.

PENALTIES

The SEC imposed significant civil penalties on the four companies, totaling $7 million, with the lowest fine at $990,000 and the highest fine at $4 million.

TAKEAWAYS

Companies should take these actions seriously and assume that they are the beginning of heightened scrutiny and enforcement by the SEC. In particular, companies should consider the following:

1. **Importance of Accurate Disclosures:** These significant penalties and related public attention highlight that it is critical for companies to provide precise and comprehensive disclosures about cybersecurity risks and incidents in annual filings as well as in their 8-K reports. While general references or language may have been less scrutinized in the early days of the disclosure requirements (or before the specific requirements were in effect), this is clearly no longer the case, particularly when describing actual incidents.
2. **Strong Disclosure Controls:** Companies should implement and maintain robust disclosure controls and procedures to promptly identify and assess the impact of cyber incidents. In the event of a security incident, legal counsel should be prepared to work closely with security teams to ensure accurate reporting and to evaluate the potential materiality and impact of a particular incident or series of incidents. These reporting requirements and procedures should be clearly set out in the company's incident response plan and specific guidance should be developed for evaluating materiality in this context.

3. **Regulatory Compliance:** Staying abreast of regulatory requirements and guidance from the SEC is crucial, as the SEC's oversight and guidance is still evolving. Companies should review and document best practices for cybersecurity disclosures to avoid potential penalties and reputational damage. They should also benchmark their own disclosures to those of other similarly situated organizations, while keeping in mind that more limited or general disclosures may not longer hold up to SEC scrutiny even if still common in the market.

4. **Proactive Risk Management and Review:** Companies must be proactive in their approach to mitigating and responding to cyber risks to help prevent incidents before they occur as well as mitigate the impact of incidents that do occur. These steps include the preparation and deployment of tailored incident response policies and procedures as well as conducting regular risk assessments, employee training through tabletop exercises, and incident response planning. These steps are also critical for companies to ensure that their cyber security infrastructure is accurately reflected in the descriptions included in their public disclosures.

The SEC has fired a significant shot over the bow, and companies should take this as a reminder that these enforcement actions are almost certainly a sign of additional scrutiny and enforcement over the coming months. This action also comes at a time when security incidents and data breaches pose an ever-increasing threat to all organizations, such that companies must assume that they may face a material incident at any time and prepare accordingly.

RELATED PRACTICE AREAS

- Data Privacy & Security
- Securities & Corporate Governance

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Andrea Rastelli

Boulder

andrea.rastelli@bclplaw.com
+1 303 417 8564