Articles + Publications | August 6, 2024

SolarWinds Ruling Offers Cyber Incident Response Takeaways

WRITTEN BY

Jay A. Dubow | David I. Meyers | Sadia Mirza | Ghillaine A. Reid | Casselle Smith

A federal judge in New York has issued a devastating blow for the U.S. Securities and Exchange Commission's high-profile cybersecurity case against SolarWinds Corporation and its chief information security officer, Timothy Brown.[1]

On July 18, U.S. District Judge Paul A. Engelmayer of the U.S. District Court for the Southern District of New York issued a 107-page opinion and order dismissing all charges related to the 2019 Sunburst cyberattack that triggered the SEC's underlying investigation of SolarWinds.[2] But neither the company nor its CISO are off the hook just yet, as one aspect of the SEC's case against them remains.

Specifically, the court sustained the SEC's securities fraud charges based on allegedly false and misleading statements contained in a "security statement" that the company provided to its customers and posted on its public-facing website in 2017, prior to the cyberattack.

It is still too early to determine what, if any, effect this order will have on the growing muscularity of the SEC's cybersecurity enforcement program. However, Judge Engelmayer's well-reasoned decision offers rich insight into the factors that companies should consider when examining their public disclosures and testing their incident response plans.

Background on the Sunburst Attack

In December 2020, SolarWinds learned of a large-scale cyberattack targeting its flagship product — the Orion software platform. This cyberattack, known as Sunburst, has been attributed to a group of threat actors sponsored by the Russian Foreign Intelligence Service, and is widely considered one of the worst cyberespionage campaigns in U.S. history.

The SEC alleges the threat actors were able to exploit SolarWinds' known cybersecurity weaknesses to access the company's corporate VPN and then remain in its systems undetected for nearly two years.[3] According to the SEC, the threat actors gained access to SolarWinds' "entire network" and were able to "elevate privileges, disable antivirus software, and access and exfiltrate data, including computer code and customer information, without triggering alerts from SolarWinds' data loss prevention software."[4]

The threat actors inserted malicious code into several Orion builds, which went out as updates to approximately 18,000 SolarWinds customers, and created a backdoor for the threat actors to access those customers' systems.[5]

In June 2021, the SEC undertook a massive sweep to, among other things, identify the scope of Sunburst's effect on SEC-regulated entities. In its complaint against SolarWinds and Brown, the SEC asserts that Sunburst affected "numerous federal and state government agencies, and more than 1,500 publicly traded U.S. companies, banks, broker-dealers, accounting firms, and other entities regulated by the SEC."[6]

Additionally, according to the SEC, the threat actors used the Sunburst backdoor to conduct secondary attacks on approximately 100 companies and government agencies.[7]

The SEC's Charges Against SolarWinds and its CISO

In October 2023, the SEC filed an enforcement action in federal court charging the defendants with scienter-based securities fraud, false filings with the SEC, and internal controls violations.

The SEC amended its complaint in February 2024 to include additional support for its allegations that both SolarWinds and Brown were aware of the company's significant cybersecurity deficiencies prior to the Sunburst attack.

In sum, the SEC's enforcement action was based on allegations that:

The company had known for years that its deeply flawed cybersecurity apparatus left its critical assets overly vulnerable to attack;[8]

At Brown's direction and with his approval, the company created a materially false and misleading security statement to use as its official response to cybersecurity questionnaires from its customers;[9]

The company's pre-Sunburst public statements — in presentations, podcasts, blog posts and press releases — and filings with the SEC misled investors to believe SolarWinds had robust cybersecurity practices;[10]

The current reports on Form 8-K filed by SolarWinds in the immediate aftermath of Sunburst misled investors by minimizing the attack's scope and severity;[11] and

The company's internal controls related to cybersecurity were materially deficient.[12]

The Court's Ruling on Defendants' Motion to Dismiss

The court sustains the fraud claims based on the security statement.

The court sustained the SEC's scienter-based securities fraud claims related to the security statement posted to the company's website in 2017, ruling that the SEC viably pled that the security statement was "materially false and misleading in numerous respects";[13] and "that SolarWinds and Brown acted with scienter in keeping the

Security Statement on the company website in the face of known cybersecurity deficiencies that made the statement false and misleading."[14]

The court emphasized that the soundness of SolarWinds' cybersecurity practices is critical to its reputation as a software company, and the materiality of the security statement was evident in how the company leveraged it to respond to vendor questionnaires.

Even though the security statement was directed at customers ?— not investors ?— the court found that it was "unavoidably part of the 'total mix of information' SolarWinds furnished to the investing public."[15]

Judge Engelmayer opined that "a reasonable person contemplating investing in SolarWinds would have viewed the alleged gap between SolarWinds' words and on-the-ground reality as highly consequential — as 'significant in making investment decisions.'"[16]

The court dismisses the fraud and false filings charges based on other disclosures.

The court rejected the SEC's allegations that defendants' other pre-Sunburst public statements in blog posts, podcasts and press releases were materially false and misleading to investors.

Unlike with the company's security statement, the court ruled that each of these other public statements "qualifies as non-actionable corporate puffery, too general to cause a reasonable investor to rely upon them."[17]

The court also rejected the SEC's contention that SolarWinds' cybersecurity risk disclosures ?— contained in the company's registration statement and periodic filings with the SEC? — were unacceptably boilerplate and generic. Instead, the court found that they sufficiently alerted the investing public of the types and nature of the company's cybersecurity risks, as well as the grave consequences those risks presented for the company's financial health and future.[18]

Finally, the court rejected the SEC's arguments regarding the Form 8-K filed just days after the company learned of the Sunburst attack, ruling that those charges impermissibly relied on hindsight and speculation. The SEC failed, in the court's view, to plead with particularity that these disclosures — which "captured the big picture"[19] and "bluntly reported brutally bad news for SolarWinds"[20] — misled investors by omitting details about certain aspects of the attack.

The court dismisses the alleged internal controls violations.

The court also dismissed the SEC's claim that SolarWinds' disclosure controls were ineffective. That charge was based on allegations that SolarWinds erroneously classified two events as a level 0 under its cyber incident response plan. At the time, the company had not yet learned of the Sunburst attack and was unaware that these earlier incidents were connected.

The court ruled that the company's incident response plan — as pled in the SEC's complaint — was designed to ensure that material cybersecurity information was timely communicated to the executives responsible for the company's public disclosures. The court explained that errors can occur without systemic deficiencies, and that

these two misclassifications were insufficient to plead a disclosure controls violation.

The SEC attempted to expand its authority to regulate registrants' practices by arguing that SolarWinds' deficient cybersecurity practices violated Section 13(b)(2)(B) of the Securities Exchange Act, which requires that public companies implement internal accounting controls sufficient to safeguard corporate assets from unauthorized use.

The SEC acknowledged this was its first time bringing a contested Section 13(b)(2)(B) charge based on cybersecurity controls, and the court dismissed it as a matter of law. The court noted that the statute — which was passed as part of the Foreign Corrupt Practices Act — can only be used to govern "internal accounting" controls and cannot be expanded to cover every internal system a public company uses to guard its assets.

However, SEC has settled with parties that it alleged violated the internal accounting and disclosure controls provisions in actions involving cybersecurity incidents.

Legal Implications and Practical Guidance

The court's order is no doubt devastating for the SEC's enforcement action against SolarWinds and Brown. Other companies and their officers will leverage Judge Engelmayer's decision to push back on potential SEC enforcement actions involving findings similar to the ones dismissed in this case, especially as it relates to the SEC's use of Section 13(b)(2)(B).

Nevertheless, the SEC will continue to bring cases involving cybersecurity disclosures. This is just one district court decision, and other courts may rule differently. Moreover, this case involves incidents that occurred prior to the SEC's adoption of new cybersecurity rules in July 2023, which created an entirely new basis upon which the agency can charge companies for cybersecurity-related disclosures.

When viewed against this landscape, one of the order's most important takeaways is not in what the court dismissed, but what it sustained — the SEC's scienter-based securities fraud charge ?— against both the company and its CISO, based on the security statement.

In the wake of catastrophic cyberattacks, software developers and other IT companies should expect the SEC to closely scrutinize their public representations regarding the soundness of their cybersecurity practices — even when those statements are not directed at investors. This is particularly true for incidents that regulators may perceive as arising from known gaps that contradict the company's prior public statements regarding its cybersecurity practices, and that have significantly affected the company's stock price.

Several valuable lessons from the court's decision — if acted upon, can improve a company's defensive posture in the wake of a major incident.

1. Review public statements through the investor lens, even when they are not the intended audience.

The court's order clarifies that, while certain public statements may be considered mere "corporate puffery," other representations on a company's website — such as policy statements, white papers, and other concrete representations regarding the specific nature of the company's cybersecurity practices — may be material to

investors.

Publicly available marketing materials must be meticulously reviewed, by both security and legal teams, to ensure accuracy and consistency, and to avoid committing the company to obligations that would not otherwise be imposed.

For example, claiming to comply with “industry standard best practices” is an unforced error, as it implies the company is adhering to a comprehensive standard that does not exist. In reality, there is no single cybersecurity standard that applies to all businesses. Instead, there are various frameworks and guidelines ?— e.g., the National Institute of Standards and Technology Cybersecurity Framework and Center for Internet Security Controls ?— that help companies design information security programs tailored to their unique risks and needs.

While certain laws may prescribe specific types of controls, they do not constitute a comprehensive standard addressing cybersecurity holistically. Therefore, statements about cybersecurity must be carefully crafted to accurately reflect the company’s cybersecurity program, recognizing that these documents can act as a double-edged sword.

2. Periodically audit incident severity classifications under existing incident response plans.

As part of incident response planning and management, security teams often rely on a formalized triage process to establish the necessary escalation and response for each incident. For example, security teams may be required to assign a severity level to each incident on a scale from 1 to 4 — with Level 1 being routine incidents manageable by internal IT members without further escalation, and Level 4 being major incidents requiring a comprehensive response.

While the court rightly acknowledges that some misclassifications are inevitable, its ruling underscores that a company’s systemic failure to assign appropriate severity levels could constitute an actionable disclosure controls violation. Similarly, a company’s routine failure to reevaluate severity levels as facts on the ground develop could also lead to disclosure issues.

Companies should consider implementing systems, such as an internal audit process, to ensure their security teams are properly assigning and updating severity classifications, and that incidents are being escalated to the company’s disclosure decision makers accordingly.

If a company identifies multiple misclassifications through an internal audit, it should document the steps taken to address those miscalculations, how the company responded to them at the time, and what changes were made to existing processes and procedures to prevent future occurrences. Companies that proactively look for and remediate misclassification issues may receive more favorable treatment from regulators than those that do not.

---

[1] SolarWinds is a Texas-based company that develops and sells network monitoring software used by over

300,000 governmental and private entities, including 499 of the Fortune 500. The company hired Brown, in 2017 and completed an IPO the following year and begin trading on the New York Stock Exchange.

[2] Opinion & Order, *SEC v. SolarWinds Corp. and T. Brown*, 1:23-cv-09518-PAE (S.D.N.Y. July 18, 2024) (Order).

[3] Amended Complaint at ¶253.

[4] Order at 27.

[5] See Order at 28.

[6] Order at 28.

[7] Amended Complaint at ¶258.

[8] See Order at 11.

[9] Order at 6.

[10] Order at 10.

[11] Order at 2.

[12] Order at 3.

[13] Order at 3.

[14] Order at 61.

[15] Order at 51.

[16] Order at 59.

[17] Order at 68.

[18] See Order at 72.

[19] Order at 90.

[20] Order at 88.

RELATED INDUSTRIES + PRACTICES

- Incidents + Investigations

- Privacy + Cyber
- White Collar Litigation + Investigations