BCLP. Client Intelligent

**BCLPSecCorpGov.com**

# SEC BRINGS LANDMARK CYBERSECURITY DISCLOSURE LAWSUIT AGAINST SOLARWINDS AND ITS CISO

Nov 01, 2023

On October 30, 2023, the SEC filed charges against SolarWinds Corp. and its chief information security officer (CISO), alleging:

- Failures to disclose known cybersecurity vulnerabilities affecting the company's "crown jewel" products.
- Failure to disclose red flags following attacks against two customers.
- Following discovery of a third incident, failure to disclose the fact that the vulnerability had been exploited on multiple previous occasions.

The SEC's complaint alleged that:

- SolarWinds and the CISO violated the antifraud provisions of the federal securities laws.
- SolarWinds violated reporting and internal controls provisions of the Exchange Act.
- The CISO aided and abetted the company's violations.

The complaint seeks permanent injunctive relief, disgorgement with prejudgment interest, civil penalties, and an officer and director bar against the CISO.

## TAKEAWAYS

The charges come less than two months before the effective date of the SEC's new cybersecurity rules, which require prompt Form 8-K reporting of material cybersecurity incidents and annual disclosure of cybersecurity risk management, strategy and governance. Together they illustrate the SEC's heightened focus on this area. The Director of the SEC's Division of Enforcement stated that this enforcement action "underscores our message to issuers: implement strong controls calibrated to your risk environments and level with investors about known concerns."

In light of the new rules and the enforcement action, and in addition to the recommended actions in our July 2023 post, companies should:

- Evaluate controls and procedures to ensure that potentially material cybersecurity issues are properly considered by management and the law department, including internal reporting within information security teams.
- Evaluate the company's internal culture to ensure that employees recognize the importance of treating cybersecurity issues with appropriate seriousness.
- Review security statements on company websites, product materials and similar communications to make sure they are balanced and do not overstate their functionality or lack of vulnerability.
- Monitor internal documentation, including emails, messages and presentations, and promptly address and/or resolve any red or yellow flags.
- Remind employees about proper email and messaging practices, such as avoiding gossip, irreverent comments or other content that can be misconstrued in an investigation or litigation.

## DEEPER DIVE

The SEC alleged that, from the IPO of SolarWinds in October 2018 through January 2021, the company and its CISO defrauded investors and customers through misstatements, omissions, and schemes that concealed its poor cybersecurity practices and its heightened— and increasing— cybersecurity risks.

The company provided software to companies and government agencies to manage their information technology infrastructure by, for example, monitoring activity on networked servers.

The SEC alleged that the company's poor controls, false and misleading statements and omissions would have violated the federal securities laws "even if SolarWinds had not experienced a major, targeted cybersecurity attack. But those violations became painfully clear when SolarWinds experienced precisely such an attack."

The complaint stated:

> "The true state of SolarWinds' cybersecurity practices, controls, and risks ultimately came to light only following a massive cyberattack—***which exploited some of SolarWinds' poor cybersecurity practices***—and which impacted thousands of SolarWinds' customers. That attack, termed SUNBURST, compromised SolarWinds' Orion software platform, a flagship product that the Company considered to be a "crown jewel" asset and which accounted for 45% of its revenue in 2020."

## THE SUNBURST ATTACK

As early as June 2018, SolarWinds had a known vulnerability that allowed access to the company's virtual private network ("VPN") through unmanaged devices such as cell phones and laptops that were neither owned nor operated by the company. In January 2019, threat actors – later identified as the Russian Foreign Intelligence Service – accessed its systems through the VPN using an unmanaged device, exploiting a vulnerability identified by a company engineer six months earlier but which was neither remediated nor disclosed.

The actors then had broad, undetected access to SolarWinds' systems. Using their access, they 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. They were also able to access and monitor network access and emails of SolarWinds' key personnel without detection.

Eventually, they inserted malicious code into three software builds for SolarWinds' Orion products. SolarWinds then delivered these compromised products to more than 18,000 customers across the globe. The malicious code provided the threat actors with the ability to access the systems of these compromised customers, provided certain other conditions were met, and became known as the SunBurst attack. Affected customers included 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. The Government Accountability Office published an overview here.

After attacks on several customers, the company filed an 8-K disclosing that its Orion network monitoring software contained malicious code that had been inserted by threat actors as part of a supply-chain attack and "could potentially allow an attacker to compromise the server on which the Orion products run." It also indicated that it was still investigating whether and to what extent a vulnerability was exploited. The SEC alleged that the 8-K was materially misleading because it failed to disclose that the vulnerability had been actively exploited multiple times over at least the past six months against several customers.

SolarWinds' stock price dropped more than 25% over the two trading days after it announced the SunBurst attack. The stock price continued to drop and lost approximately 35% of its value by the end of the month as SolarWinds disclosed more details of the SunBurst attack.

## KNOWN CYBERSECURITY VULNERABILITIES

The SEC alleged that the CISO and other employees were aware of "pervasive" cybersecurity deficiencies, based on internal emails, messages and documents that "dramatically contradict SolarWinds' public disclosures." These included, among others:

- An email admitting that "***we don't do*** some of the things that are indicated in the [Security Statement's SDL section]."
- A statement by an engineer that the company's remote access VPN was "not very secure" and that someone exploiting the vulnerability "can basically do whatever without us detecting it until it's too late" which could lead to a "major reputation and financial loss." for SolarWinds.
- A presentation by the CISO contemporaneous with its IPO stating that the "[c]urrent state of security leaves us in a very vulnerable state for our critical assets" and that "[l]ack of cyber hygiene leaves us open to being a target of opportunity."
- A presentation by the CISO to senior management warning that "[a]ccess and privilege to critical systems/data is inappropriate"
- A presentation to the CISO stating that there was "No true expertise for security" and that core teams "do[] NOT understand security!"
- Presentations highlighting "[s]ignificant deficiencies" in access controls.
- An email to the CISO that "we have a systemic issue around lack of awareness for Security/Compliance requirements with most if not all DOIT projects."
- In response to alarm expressed by engineer at activity at a customer, the CISO acknowledged the incident was "very concerning" and stated, "As you guys know our backends are not that resilient and we should definitely make them better."
- A warning that "[t]he volume of security issues being identified over the last month have outstripped the capacity of Engineering teams to resolve."
- A manager messaging that "[W]e're so far from being a security minded company. [E]very time I hear about our head geeks talking about security I want to throw up."

The SEC alleged that the specific cybersecurity issues identified in the complaint "were part of a pervasive cybersecurity problem throughout SolarWinds" and "reflected a culture that did not take cybersecurity issues with sufficient seriousness."

## MATERIALITY

The SEC alleged that a reasonable investor would have considered it important to know:

- The true nature and scale of the cybersecurity risks facing the company, not merely generic risk disclosures.

- The company's known and increasing risk of cyberattacks, which could have materially negative effects on the company.

While cybersecurity is important for all public companies, the SEC alleged that "they are especially important for a company like SolarWinds whose primary product is not only software, but software that other organizations install to manage their own computer networks."

The SEC highlighted that Orion represented 45% of SolarWinds' revenue in 2020 and there were multiple red flags suggesting both intrusions at SolarWinds and specific problems with Orion. The attacks also affected SolarWinds' MSP products, another "crown jewel."

The SEC alleged that the materiality of the issues was heightened by the presence of other issues, noting, for example, the increased materiality of SolarWinds having both the VPN issue and the pervasive use of admin rights.

## FALSE AND MISLEADING STATEMENTS

The complaint alleged false and misleading statements and omissions were made in several types of public disclosures:

**Website security statement.** The company touted its purportedly strong cybersecurity practices in a website statement, including:

- That the company followed the principal industry (NIST) framework for evaluating cybersecurity practices -- even though it had no program or practice in place for the majority of controls specified in the framework.
- That its software products were created in a "secure development lifecycle [that] follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments" -- even though the CISO and other engineers acknowledged they were still establishing a plan to implement those practices.
- That its "password policy covers all applicable information systems, applications, and databases [and we] enforce the use of complex passwords" -- even though the CISO and others knew that password problems had persisted for years, including lack of encryption and storage in plain text.
- That its "[a]ccess controls to sensitive data in our databases, systems, and environments [that are] set on a need-to know/least privilege necessary basis" -- even though the CISO and management knew the company frequently granted employees unnecessary "admin" rights and failed to enforce its remote access for its VPN.

**SEC filings.** The SEC alleged that the company and CISO also repeatedly made misleading disclosures in the Form S-1 for its IPO, Form S-8s as well as 10-Ks and 10-Qs, including:

- General high-level risk disclosures that lumped cyberattacks in a list of risks alongside “natural disasters, fire, power loss, telecommunication failures…[and] employee theft or misuse.”
- Cybersecurity risk disclosure was generic and hypothetical, allowing for negative consequences “[i]f we sustain system failures, cyberattacks against our systems or against our products, or other data security incidents or breaches.”
- Failing to address known risks, particularly that the company had already determined that it was not taking adequate steps to protect against anticipated and known risks, including failing to follow the steps outlined in the Security Statement.

The company did not disclose these issues, even during the period when it became aware of red flags indicating it had been, or was at increased risk of soon becoming, the target of a significant cyberattack, including as a result of reports of cyberattacks by two customers and subsequent investigations by the company.

The SEC also alleged that the 8-K filed on December 14, 2020 (reporting that its Orion network monitoring software contained malicious code) was materially misleading because it failed to disclose that the vulnerability had been actively exploited multiple times over at least the past six months against several customers.

**Informal communications.** The SEC also cited allegedly misleading disclosures by the CISO, on behalf of the company, regarding its cybersecurity “best practices” and “high security standards” in other communications, including podcasts, blog posts, and press releases.

## RELATED PRACTICE AREAS

- Securities & Corporate Governance

## MEET THE TEAM


**R. Randall Wang**

St. Louis

randy.wang@bclplaw.com
+1 314 259 2149



**Eliot W. Robinson**

Atlanta

eliot.robinson@bclplaw.com
+1 404 572 6785


---