GT GreenbergTraurig

Alert | Data Privacy & Cybersecurity/ Financial Regulatory & Compliance

November 2023

Chief Information Security Officers in SEC Crosshairs: The SolarWinds Case

Go-To Guide:

- On Oct. 30, 2023, the SEC filed its first case against a public-company Chief Information Security Officer (CISO) after the well-published SolarWinds Corp. "SUNBURST" cyberattack.
- The SEC alleges that the CISO, from SolarWinds October 2018 initial public offering through the company's December 2020 announcement of the SUNBURST cyberattack, defrauded investors by overstating SolarWinds' cybersecurity practices and understating (or not disclosing) known cyber risks.
- According to the SEC, SolarWinds' public statements about its cybersecurity practices and risks did not square with internal assessments shared with the CISO, as well as the CISO's own presentations about the company's cyber vulnerabilities.
- The SEC complaint, filed in the Southern District of New York, alleges the CISO violated the anti-fraud provisions of the Securities Act of 1933 and Securities Exchange Act of 1934, and seeks permanent injunctive relief, disgorgement, civil penalties and an office and director bar against him.

In a Halloween-eve move sure to send shivers down the spines of every public company's CISO, on Oct. 30, the SEC filed a securities fraud complaint targeting SolarWinds' CISO in the wake of their major December 2020 data security incident. The SEC alleges SolarWinds and its CISO committed securities

fraud in connection with multiple public disclosures about its cybersecurity practices, including the form 8-K disclosing the incident. This move is the latest in a series of steps taken by the SEC to flex its muscles in regulating data security.

SolarWinds Incident

In December 2020, SolarWinds, a software security company, publicly announced that its Orion product was the target of a large-scale attack later attributed to a Russian-government-backed hacking group. The attack, which persisted for months without being detected, affected 18,000 customers, including U.S. government agencies. The Microsoft president said it was "the largest and most sophisticated attack the world has ever seen."

Complaint Allegations

The SEC's complaint names SolarWinds and its CISO as defendants. This is a serious problem for CISOs generally, as it puts them directly and personally in the crosshairs of a regulatory agency with the authority to both fine them personally and prevent them from ever holding a senior position within any public company.

The SEC identifies three areas where SolarWinds and the CISO allegedly made materially false statements about information security: (1) in a Security Statement on SolarWinds' website; (2) in publicly filed Forms S-1 and 10-K and 10-Q; and (3) in the 8-K filed after the December 2020 disclosure of the security vulnerability.

The SEC's complaint cites to numerous presentations and internal emails and chats where employees made multiple statements that directly contradicted the Security Statement, which contained detailed information about SolarWinds' data security practices. The SEC is specific about a few areas where it alleges SolarWinds committed violations: (1) secure development lifecycle; (2) password management; and (3) least access privilege. The SEC points to documents and communications it alleges show an awareness *at the time* by people at SolarWinds that these representations were not true, including internal communications suggesting that the Security Statement itself was false. For example, the Security Statement claimed SolarWinds followed security standards published by the National Institution of Standards and Technology (NIST). The SEC says that security assessments SolarWinds performed showed it was far from compliant with NIST.

With respect to SolarWinds' public SEC filings, including its S-1 initial public offering and its quarterly and annual 10-Q and 10-K filings, the SEC accuses SolarWinds and its CISO of misleading investors by omitting known cybersecurity risks, relying instead on generic statements about potential cybersecurity risks. The SEC states, "those risks are not being assessed in hindsight by the SEC. [The CISO] and others at SolarWinds assessed and documented them at the time. Indeed, as [the CISO] stated (internally) during the very month that SolarWinds made the above public disclosure: the 'current state of security leaves us in a very vulnerable state for our critical assets.'" Similar generic statements were contained in 10-Ks and 10-Qs up until November 2020. The SEC says the statements became more misleading and falser over time as SolarWinds began receiving customer complaints of malicious activity throughout 2020.

With respect to the incident itself and statements in SolarWind's 8-K filing concerning the incident, the SEC calls out SolarWinds and the CISO for understating the risks known to them at the time. When the 8-K was filed, the SEC claims it was materially misleading in three ways:

- It said the cyberattack "could potentially allow" a data compromise, when SolarWinds allegedly knew this was not theoretical but rather the attacker had already compromised the server and had already utilized the vulnerability with three different customers since May 2020;
- It said SolarWinds was doing an investigation including "whether a vulnerability in the Orion monitoring products was exploited," when in fact SolarWinds knew it had been exploited at least three times.
- It said SolarWinds was "still investigating whether, and to what extent, a vulnerability in the Orion products was successfully exploited," when the SEC claims SolarWinds and its CISO had specific knowledge that had already happened.

The SEC says the CISO participated in the meeting when the statement was drafted and he reviewed and confirmed its accuracy, despite knowing that the three different customer attacks were connected. If true, this is a serious allegation of scienter, i.e., proof of a mental state embracing the intent to deceive, which includes deliberate recklessness or an extreme departure from the standard of care. The SEC has also alleged negligence-based charges, which require a lower standard of proof because intent is not required.

The SEC has a formidable arsenal of weapons in the form of relief it can seek in its enforcement actions. Typically, it will seek a permanent injunction against future violations of the securities laws, disgorgement of ill-gotten gains (with pre-judgment interest), civil monetary penalties, and an order permanently prohibiting a defendant from acting as an officer or director of publicly traded companies. In plain English, should the SEC prevail in its action against the CISO, it could end his career as a CISO for any publicly traded company, as well as trigger significant financial consequences for him individually. The personal and professional stakes could not be higher for CISOs.

Takeaways

- The SEC's complaint puts public company CISOs directly in the crosshairs. Therefore, CISOs in their employment agreements will likely seek to get companies to agree to pay for legal fees and indemnify them (if possible) from any such actions. Companies may need to review their D&O insurance coverage to determine if they would provide protection for CISOs in the event of a regulatory investigation or litigation.
- Companies should consider reviewing all public statements about their security posture to make sure they are supported by the evidence; this includes any security statements provided in customer agreements. Because there is sometimes a disconnect between the employees who draft these documents, which are often more sales/marketing in nature, and those who handle security, there should be clear lines of communication across functional areas and business units.
- Companies will need to make sure that the CISO reviews 10-Ks and 10-Qs to ensure they do not omit or understate known risks. Because every company has some security gaps, it could create risk for a company if they publicly disclose those gaps (threat actors read public filings too).
- If a company has an incident and needs to file an 8-K – which is now expressly required under the recently finalized SEC cybersecurity rules for public companies – it is important to be specific about what the company actually knows at the time. The SEC has fined investment advisors for similar misstatements. The new rule requires public companies to file an 8-K within four business days of determining materiality in the event of a cybersecurity incident (an analysis itself sure to cause heartburn). Although the SEC has acknowledged that companies may still be investigating an incident, and therefore many facts may not yet be known, the allegations against SolarWinds suggest a more aggressive approach. Companies may find themselves stuck between a rock and hard place – if they are

too definitive in their disclosures and facts change, or if they aren't definitive enough, they could be accused of misleading investors. Regardless, an updated 8-K should be filed to disclose any information unavailable or later found to be incorrect at the time of the initial filing.

- Companies need to have more transparent communication between the CISO and executive leadership and the board. The complaint suggests that the CISO wasn't keeping management appropriately informed of the risks. Whether this is a fair assessment of what was happening is to be determined, but the new SEC cybersecurity rule explicitly requires companies to disclose in their 10-Ks how management and the board are overseeing cybersecurity risks.
- Companies must be careful when hiring third-party consultants to do security assessments. The reports of these assessments often read like a roadmap of where a company is falling short – in the consultant's view – of a fulsome cybersecurity program. Those can be later used against a company in an investigation of their public disclosures.
  - Prior to obtaining a written report from the consultant, companies should ensure that they agree with the identified gaps and/or can provide additional information that might impact the findings.
  - If the information security team disputes any report findings or if they have compensating controls not reflected in the report (i.e., the finding is accurate, but the impact is blunted by a different security measure), they should prepare a rebuttal memo contemporaneously documenting that additional information. An ex post facto review may be too late to be of benefit.
  - Any critical or high vulnerabilities should be remediated immediately. While this may obvious, companies sometimes complete an assessment but never follow through with a remediation plan. Any such plan and its completion should be documented.
  - Involvement of legal counsel can result in a privileged and focused analysis of improvements companies can make to their cybersecurity posture to reduce liability for similar investigations and litigation.
- Companies should consider regular training around what is appropriate to say in an email or on a Teams chat. Multiple statements cited in the SEC's complaint came from informal discussions over email or chat where employees may have felt it was a "safe" channel of communication.
- Companies should consider creating a reporting chain where lower-level employees feel empowered to share concerns with someone in management who isn't the CISO. That way management can learn of identified risks without relying on a single person to be the gatekeeper for those communications.

Authors

This GT Alert was prepared by:

- Jena M. Valdetero | +1 312.456.1025 | Jena.Valdetero@gtlaw.com
- Steven M. Malina | +1 312.476.5133 | Steven.Malina@gtlaw.com