Cooley

Fatal Flaws in SEC's Amended Complaint Against SolarWinds

April 17, 2024

In March 2024, **a coalition of more than 50 cybersecurity leaders and organizations called for dismissal** of an amended complaint by the Securities and Exchange Commission (SEC) against SolarWinds and its chief information security officer (CISO), Tim Brown. Amici from the business community and the software industry, as well as former law enforcement officials, joined the cybersecurity coalition's push, arguing that the SEC's latest allegations against SolarWinds and Brown – the first time in history that the SEC has charged a CISO with securities violations – are counterproductive for cybersecurity and national security.

The SEC's continued pursuit of charges, notwithstanding the chorus of dissent by cybersecurity, business and government leaders, highlights the stakes of this bellwether case for cybersecurity policy nationwide. The SEC's charges also provide a stark warning for companies, executives and cybersecurity professionals that the SEC remains committed to policing cybersecurity in the years to come.

Case background

In October 2023, the **SEC charged SolarWinds and its CISO with alleged securities violations** based on the company's public statements and SEC disclosures before, during, and after a two-year-long Russian government-backed cyberattack campaign (dubbed "SUNBURST") against SolarWinds. This was the first time that a CISO faced charges for alleged cybersecurity misrepresentations in a company's SEC filings.

SolarWinds and Brown moved to dismiss the SEC's complaint in late January. In addition, in a rare showing of support at the motion to dismiss stage, four groups of interested parties filed amicus briefs in early February raising significant policy concerns with the SEC's charges. A **coalition of CISOs, cybersecurity professionals and cybersecurity organizations, represented by Cooley** (including the authors of this post) and Freshfields Bruckhaus Deringer US, argued that the SEC's theories of liability were "counterproductive given the real-world demands of cybersecurity, and risk harmful consequences, including elevating the frequency and harm of cyberattacks, impeding internal efforts to bolster cybersecurity, worsening the CISO hiring and retention crisis, and deterring CISOs from cooperating" with the government. BSA The Software Alliance, an industry group, **filed a brief making similar arguments from the perspective of software companies**.

In another amicus brief, **former law enforcement officials stressed** that the SEC's theories could make companies more reticent to voluntarily share information with law enforcement, hampering government efforts to combat cyberthreats. And **the US Chamber of Commerce and Business Roundtable** argued that the Securities Exchange Act of 1934, which governs corporate financial controls and is central to the SEC's charges, was never intended to reach cybersecurity practices.

Latest developments

On February 16, 2024, **the SEC withdrew its original allegations and filed an amended complaint** containing more detailed factual allegations against Brown and responding to some of the arguments made by amici. For example, amici argued that the SEC's charges against SolarWinds and Brown were, in effect, an effort to impose new requirements on CISOs just as other government organizations were highlighting the importance of flexibility in the CISO role. But in the second paragraph of **its amended complaint**, the SEC insists: "This is not a case about isolated failures, attempts at compliance that were good but less than perfect, or the SEC seeking to impose its own set of specific cybersecurity protocols on SolarWinds or all public companies."

SolarWinds and Brown filed a renewed motion to dismiss on March 22. According to their motion, the SEC's amended allegations are "**an attempt to find some theory to hold its case together**" and are "contradicted by the very documents on which the mended omplaint relies."

The latest filings by amici on March 29 echoed the concerns raised in their original briefs supporting dismissal filed before the SEC amended its complaint. Notably, the cybersecurity coalition filed a renewed amicus brief signed by 50+ cybersecurity heads, including more than 20 new individuals who joined after the earlier filing. Other amici groups rested

on their previous filings. As **BSA explained in a letter to the court**, the amended complaint "advance the same core theory of liability set forth in original complaint … which will have the same troubling implications for cybersecurity described in BSA's brief." Below is summary of several of the main areas of dispute – all of which highlight the challenges for companies and CISOs raised by the SEC's claims.

Amici's concerns with amended complaint

First, in an apparent effort to justify claims based on statements about security, the SEC's amended complaint adds comments from investors, including a large pension fund and securities analysts, stating that SolarWinds's representations about cybersecurity were material in their investment decisions and recommendations. The amended complaint also relies heavily on statements made by SolarWinds outside the company's SEC filings, citing its website, customer questionnaires, contracts, emails, letters, podcasts, blog posts, speeches, webinars and other publicity. Relying heavily on nonfinancial public statements highlights the Chamber of Commerce's concern that "the SEC has attempted to position itself as a super-enforcer of corporate behavior well beyond the bounds of federal securities laws."

Second, the SEC's amended complaint alleges additional allegations of noncompliance with SolarWinds' cybersecurity policies (e.g., access controls, password rules, employee trainings, incident response plans) and/or certain frameworks (e.g., National Institute of Standards and Technology frameworks). But as amici noted in their initial briefs, basing liability on failure to adhere to an internal security policy or flexible cybersecurity frameworks may discourage companies and CISOs from adopting such policies and conducting self-assessments to improve their practices. Amici stressed that adopting corporate cybersecurity policies – and using those policies to identify and correct noncompliance – is essential to good cybersecurity hygiene.

Third, the SEC's amended complaint adds detail about SolarWinds' internal communications concerning cybersecurity risks, including discussions among cybersecurity employees, presentations and warnings from cybersecurity professionals to corporate leadership, and even incident response communications with customers affected by a cyberattack. These details, the SEC maintains, belie the company's external statements to customers and the public. But, just as software industry and former law enforcement official amici raised in their initial briefs, using internal discussions enforcing cybersecurity compliance as a basis for liability could chill both "candid internal deliberations" and "voluntary disclosure by companies or CISOs, who may become more cautious when considering how their communications … might increase future liability." As **the renewed CISO brief** put it, "ybersecurity professionals should not have to consult lawyers before sending an email."

Fourth, the SEC's amended complaint continues to assert that SolarWinds's internal identification of cybersecurity gaps – such as through risk reviews or other self-assessments – could have been a basis for liability even if SUNBURST had never happened. But as the renewed CISO brief pointed out, CISOs and their teams triage countless cybersecurity risks under "dynamic situations with incomplete information and no guarantee of perfect security" and identify hundreds of new risks as part of their day-to-day job functions. Amici warned that diverting scarce resources away from addressing gaps that CISOs find most critical and toward disclosing all newly identified risks can be counterproductive to cybersecurity.

Fifth, the SEC's amended complaint asserts that SolarWinds should have disclosed any cybersecurity gaps and incidents "at roughly comparable level of technical detail" as the company's other cybersecurity statements, apparently in response to amici's concerns that the original complaint could lead companies to disclose too much security information in a way that could benefit threat actors. The difficulty, as the renewed CISO brief warned, is that this kind of public disclosure of identified cybersecurity risks could "provide a trove of useful intelligence to threat actors interested in exploiting those vulnerabilities."

Moving forward

In short, the SEC's amended complaint suffers from many of the same critiques raised in the amicus briefs about the SEC's original complaint. Indeed, whether the SEC's case against SolarWinds and Brown proceeds past the motion to dismiss stage, the amended complaint offers a strong warning that the SEC is committed to expanding its enforcement agenda to encompass corporate cybersecurity.

As a result, companies and cybersecurity professionals should be cautious about any statements they make concerning cybersecurity. And as they go about their jobs identifying cybersecurity risks, assessing vulnerabilities and responding to cyber incidents, they should actively consider how their internal and external communications may be interpreted by the SEC, customers, investors, and the public.

AC, ¶ 72

AC, ¶ 244

AC, ¶ 45

AC, ¶ 313

AC, ¶ 12

AC, ¶ 245

Contributors

Andrew Goldstein
Bio

Josef Ansorge
Bio

Matt Nguyen
Bio

Robert Denniston
Bio
