SolarWinds and the SEC lawsuit

By John Bandler, Esq., Bandler Law Firm PLLC

NOVEMBER 21, 2023

The SolarWinds data breach is a case study that keeps giving to cyberlaw, offering discussion points relating to cybercrime, cybersecurity and more.

The recent civil complaint by the Securities and Exchange Commission (SEC) against SolarWinds is the latest milestone, adding more legal components plus a discussion of organization management including culture and communication.

The SolarWinds Orion attack — fodder for analysis

SolarWinds Corporation offers a network monitoring software called Orion which was used by tens of thousands of companies to manage their own networks. SolarWinds was breached as early as January 2019 and then the cyber attackers compromised the Orion software around December 2020. This infected software was downloaded and used by SolarWinds customers giving attackers free roam of customer networks, a compromise not detected for many months.

A culture of security and integrity is important and there can be a big gap between reality and appearance.

Orion customers included the U.S. Government and major corporations, the damages were immense and will continue, with future implications for cybercrime and national security.

All this provides fodder for discussion on four distinct areas of law:

- Securities laws when a public company makes inaccurate statements — including about cybersecurity — that affect company value and thus stock price.
- Cybersecurity legal requirements when organization cybersecurity falls below a certain standard and causes damages.
- Criminal laws violated by malicious attackers, first against SolarWinds and then against tens of thousands of other companies using the Orion software.
- International laws relating to the acts of one country conducted against or within the boundaries of another country.

The first point and the SEC complaint form our main focus here.

The SEC SolarWinds complaint in a nutshell

On Oct. 30, 2023, the SEC filed a lawsuit against SolarWinds and its Chief Information Security Officer (CISO) Timothy Brown. The civil complaint (https://bit.ly/3ujDDgY) is a good read if you have 68 pages worth of time; Reuters introduced it nicely in their article (https://reut.rs/49FxnQA) that day.

The complaint's first paragraph sums it up:

> "1. From at least October 2018 through at least January 12, 2021 ... Defendants SolarWinds and ... Brown, defrauded SolarWinds' investors and customers through misstatements, omissions, and schemes that concealed both the Company's poor cybersecurity practices and its heightened — and increasing — cybersecurity risks. SolarWinds' public statements about its cybersecurity practices and risks painted a starkly different picture from internal discussions and assessments about the Company's cybersecurity policy violations, vulnerabilities, and cyberattacks. Illustratively, in October 2018, the same month that SolarWinds conducted its Initial Public Offering through a registration statement with only generic and hypothetical cybersecurity risk disclosures, Brown wrote in an internal presentation that SolarWinds' 'current state of security leaves us in a very vulnerable state for our critical assets.'"

The complaint goes on to juxtapose several rosy public statements about excellent cybersecurity with contrasting internal statements of alarm acknowledging severe deficiencies.

Among the allegations is that a SolarWinds employee internally wrote "I just lied" after misleading a customer who was trying to pinpoint the source of a malicious compromise. The complaint alleges that SolarWinds knew or had reason to know their Orion platform was compromised (and therefore that every one of their customers was in danger) but chose to cover up the compromise rather than address it and warn their customers.

Eventually, one customer provided SolarWinds with clear proof that the Orion software was compromised and only then did SolarWinds disclose to other customers and the public what was happening, according to the complaint.

SolarWinds denies the charges and in a blog post, called the SEC complaint a misguided and improper enforcement action. It states the company will "vigorously oppose this action by the SEC." SolarWinds News, Oct. 30, 2023. See also "US SEC sues

SolarWinds for concealing cyber risks before massive hacking," Reuters Legal News, Oct. 30, 2023.

Painting a rosy picture

At the heart of this fact pattern and complaint is the thorny dilemma that companies and employees face on many fronts. How rosy a picture should we paint, and how honest should we be in our internal discussions?

On one hand, superiors, CEOs, investors, and customers like to hear that everything is going well and that everything is secure. Company marketers paint the prettiest picture of the product or service including that it is backed by smooth and efficient operations behind the scenes.

On the other hand, reality is usually much messier with cybersecurity and anything else of importance.

CISO as security officer, marketing officer, or both?

Good security is a selling point for any organization, especially an organization that sells a technology service. If an organization is going to sell its own security a likely spokesperson is the CISO.

But if good security is a selling point then the *appearance and perception* of good security is also a selling point. Perception can be manipulated with false or rosy statements while the actual state of security is harder to determine.

A culture of security and integrity is important and there can be a big gap between reality and appearance. A company could influence, pressure, or force their employees — including security officers — to help sell the *perception* of security. A company could take shortcuts by focusing on perception to the detriment of substance.

The heart of the complaint

The heart of the SEC's complaint is that SolarWinds was selling a perception of security that the substance of their security program could not back up. More bluntly, that SolarWinds lied about their security program and security measures in place.

And then — because of the underlying deficiencies — the worst-case scenario happened. A breach and compromise of SolarWinds and Orion and then the customers.

False and real lessons

CISOs are taking note of this complaint because it personally names a CISO and dissects all manner of internal and external statements by many people. Will their next blog, email, text, or slide deck be quoted from in a future complaint? What might be quoted from a hasty text or email of an employee having a bad day.

Some will think this complaint casts an improper chill upon all cybersecurity professionals and their ability to discuss nuanced security issues frankly. That the SEC has overreached and is attempting to penalize a company and their security officer for being the victim of a cybercrime — at the hands of a nation-state no less. Some may claim this complaint stands for the unreasonable proposition that all security vulnerabilities need to be publicly disclosed.

Fear, uncertainty, and doubt may manifest with statements like:

- Don't put it in writing.
- Definitely don't criticize the security program in writing.
- Don't make public positive statements about the security program.
- The system is unfair, regulators will sue us if we are not perfect or if we become victims to cybercrime.

But the real lesson here is that words, statements, and actions matter with cybersecurity, as with anything else of importance.

What companies and their employees say and do, or fail to do, matters. Inconsistencies, inaccuracies, and lies can put the company in jeopardy, especially when they relate to a demonstrable harm.

Good organizations and good regulators realize that cybersecurity (and all other areas of management) require good faith analysis of risks and options plus discussion, debate, and then decisions.

Organizations have legal responsibilities relating to cybersecurity. Any incident involving cybercrime or cybersecurity can affect company price. It follows that public statements about cybersecurity can be material to company value and stock price, especially for a technology company.

Diligence and negligence remain key touchstones

While cybersecurity comes with a host of complex technological terms (as does the SEC complaint) we can always return to good old negligence law. If the organization has a known issue to correct, it needs to be diligent in doing so.

Therefore, the touchstone for cybersecurity is:

- Be diligent, be reasonable.
- Don't be negligent or sloppy.

Diligent organizations will debate and disagree but improve

Good organizations and good regulators realize that cybersecurity (and all other areas of management) require good faith analysis of risks and options plus discussion, debate, and then decisions.

Organizations can develop bad habits. Those that cover up or deceive can leave deficiencies uncorrected for months or even years. Organizations that discourage frank conversation will develop coded channels of communication that are hard to decipher, resulting in costly misunderstandings and other harms.

There will always be areas for improvement, there will occasionally be some failures and cybercrime incidents.

Good organizations can recognize and truthfully acknowledge when improvement is needed and when failures occur. And then work to remedy the situation. Organizations should focus on doing the right thing and trust that regulators will act in the interests of justice if the situation arises.

John Bandler is a regular contributing columnist on cybercrime and cybersecurity for Reuters Legal News and Westlaw Today.

About the author

John Bandler is a lawyer, consultant, author, and adjunct professor at Elisabeth Haub School of Law at Pace University. He helps protect organizations from cybercrime, improve cybersecurity, and better manage information assets. His firm, based in New York, is **Bandler Law Firm PLLC**, and he can be reached at JohnBandler@JohnBandler.com.

This article was first published on Reuters Legal News and Westlaw Today on November 21, 2023.