Published on *The National Law Review* https://natlawreview.com

SEC Cyber Disclosure Charges Highlight Role of D&O Insurance to Mitigate Cyber Risks

Article By:

Andrea DeField

Geoffrey B. Fehling

Evan Warshauer

Following an investigation involving public companies potentially impacted by the 2020 SolarWinds software compromise, the US Securities and Exchange Commission recently charged several companies with making materially misleading disclosures regarding cybersecurity risks and intrusions. The SEC's enforcement is the latest example of "cyber as a D&O risk," underscoring the importance of maintaining robust directors and officers (D&O) liability coverage, along with cyber insurance, as part of a comprehensive liability insurance program designed to respond to cyber incidents.

Background

On October 22, 2024, the SEC charged four current and former public companies with making materially misleading disclosures regarding cybersecurity risks and intrusions related to the 2020 SolarWinds Orion hack. The SEC specifically found that each company learned in either 2020 or 2021 that the threat actor behind the SolarWinds Orion hack had accessed their systems without authorization, but that the companies negligently minimized the cybersecurity incident in public disclosures. The companies did so, the SEC contends, by framing the relevant cybersecurity risk factors hypothetically or generically when they knew the warned of risks had already materialized.

The SEC concluded that each company had violated certain provisions of the Securities Act of 1933, the Securities Exchange Act of 1934 and related rules. Without admitting or denying the SEC's findings, each company agreed to cease and desist from future violations of the cited provisions and to pay civil penalties ranging from $990,000 to $4 million.

Discussion

The recent SEC charges continue the trend of increased federal scrutiny by the SEC, DOJ and FTC following cybersecurity incidents. Individual directors and officers may also face personal liability, as regulators have targeted not just companies, but also individuals, in the wake of major cyber attacks.

In 2022, for example, Uber's former Chief Information Security Officer was criminally prosecuted and convicted by the FTC for failing to disclose a data breach during an ongoing investigation. More recently, the SEC's far-reaching case against SolarWinds and its CISO was largely truncated in a highly-anticipated ruling earlier this year, but certain charges against the CISO were allowed to proceed.

Cyber insurance remains critical for protecting all companies from the fallout of a cyber incident—regardless of their particular industry or trade. But with the staggering cost of cybersecurity events ($9.48 million on average in the US), cyber insurance limits are often quickly eroded, if not exhausted entirely, in the immediate aftermath of a cyber event. Those risks, combined with continued increase in government investigations, enforcement actions and follow-on civil and criminal claims against both companies and individuals, make complementary D&O coverage even more critical to fill any gaps and respond to traditional D&O exposures that may arise following a cybersecurity incident.

From building a comprehensive cyber and D&O insurance program to ensuring that in-house cybersecurity professionals like CISOs do not fall through the cracks in traditional policies, we have previously outlined common pitfalls and best practices to consider in addressing these risks. Being proactive and consulting with insurance brokers, outside coverage counsel and other risk professionals at the time policies are negotiated, renewed and placed can help avoid unexpected denials and maximize the chance of recovery in the event of a claim.

National Law Review, Volume XIV, Number 304