FINE PRINT

SEC's SolarWinds Litigation Expands Regulatory Cyberrisk Landscape

by Joshua Gold and Luma S. Al-Shibib

A new era of cyberrisk was ushered in with the litigation initiated by the U.S. Securities and Exchange Commission (SEC) against SolarWinds Corporation, and its chief information security officer (CISO). The SEC alleges fraud arising from failures to adequately disclose known cybersecurity vulnerabilities that ultimately resulted in a massive supply chain cyberattack.

In the case, cyber criminals were able to exploit vulnerabilities in SolarWinds' virtual private network to gain access to the software and cybersecurity company's systems. The hackers planted malware, known as SUNBURST, into Orion software products, which was then delivered to 18,000 SolarWinds' customers, thus providing the hackers with access to those customers' systems. The breach affected not only private businesses, but various cybersecurity companies that used the Orion software, as well as some key governmental agencies, including the U.S. Departments of Health, Treasury and State. The attack was not discovered and reported until December 2020, more than a year after attackers apparently first accessed SolarWinds' systems.

In its complaint, which was filed in New York federal court on October 30, the SEC alleges SolarWinds and its CISO knew for several years prior to the cyberattack that its systems were vulnerable and could be compromised even as they pronounced their systems secure. Rather than attempting to shore up the vulnerabilities, the complaint further alleges that SolarWinds misrepresented the adequacy of security controls and failed to disclose the known vulnerabilities in published corporate statements and regulatory filings, thereby misleading investors about material information.

The SEC's complaint clarifies that SolarWinds was not sued because it suffered a cyberattack, but rather because SolarWinds' poor cybersecurity controls and false and misleading statements to investors violated federal securities laws. The SEC alleges these violations included SolarWinds' incomplete and misleading disclosures in a December 2020 Form 8-k regarding the nature and true extent of the cyberattack. According to the SEC, the cyberattack merely brought SolarWinds' violations to light.

The enforcement action against SolarWinds appears to be the first instance in which the SEC has sued a victim of a cyberattack alleging intentional fraud as opposed to negligence-based misrepresentations. Additionally, it is the first time the SEC has asserted claims against a victim of a cyberattack without simultaneously entering a consent decree to settle the action. The case also represents the first time the SEC has charged an individual company executive for their role in a company's allegedly deficient cybersecurity disclosures. This is notable because the SEC complaint fails to detail the CISO's direct involvement in preparing or approving the cybersecurity disclosures in the company's allegedly false SEC filings. In a press release issued the day the enforcement action was filed, the SEC stated that the action is intended to send a message to public companies that they must implement strong cybersecurity controls and "level with investors about known concerns."

THE NEW ROLE OF REGULATORS AS CYBERSECURITY POLICE

The filing of the SolarWinds enforcement action is the latest devel-

RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com

November 2023

opment signaling the expanded enforcement role that federal and state agencies have assumed in addressing, regulating and monitoring cyber-related business risks and practices.

This summer, the SEC adopted expanded cybersecurity rules for regulated companies. Among other things, the new rules require cybersecurity incidents to be reported within four business days after they are determined to be material. Additionally, companies must identify which positions in management are responsible for assessing and managing cybersecurity risks, and describe the relevant cybersecurity expertise of those persons.

Similarly, on November 1, the New York Department of Financial Services, which oversees financial institutions such as banks, mortgage companies, investment firms, and insurance companies, published updates to its cybersecurity rules effective December 1. The updated rules require notification of ransom payments within 24 hours and provide strict provisions for corporate oversight of cybersecurity risks. Specifically, a covered entity is required to have a CISO who is individually responsible for the company's cybersecurity controls and for reporting incidents to the board of directors. Additionally, covered entities must institute multifactor authentication, conduct annual independent audits of their cybersecurity infrastructure, and implement breach detection systems.

Although the ultimate purpose of this increased regulatory landscape is to create a safer and more secure environment in which to conduct business, the new cyber regulations increase the potential liability companies and organizations may face as a result of a cyber incident. Given the heightened risk landscape for organizations (as well as their officers and directors), insurance coverage becomes a critical consideration. D&O insurance policies should offer protection against liability and defense cost reimbursement for shareholder, derivative, and regulatory lawsuits predicated on cyber breaches. Additional liability coverage may be provided depending upon the circumstances through E&O insurance policies, CGL policies, and of course cyber stand-alone insurance policies.

The expanded regulations provide a roadmap for shareholders, customers and consumers to bring derivative actions or consumer class actions against regulated businesses and their executives. Thus, organizations should review their cybersecurity procedures, address any vulnerabilities in their computer systems, and review all potentially applicable insurance policies to become familiar with the scope of their protection and determine whether additional insurance protection should be purchased. R

Joshua Gold is a shareholder in Anderson Kill's New York office, chair of Anderson Kill's cyber insurance recovery group and co-chair of the firm's marine cargo industry group. He is co-author with Daniel J. Healy of Cyber Insurance Claims, Case Law, and Risk Management, published in 2022 by the Practising Law Institute. **Luma S. Al-Shibib** is a shareholder in the New York office of Anderson Kill and co-chair of the firm's cyber insurance recovery practice group.

RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com