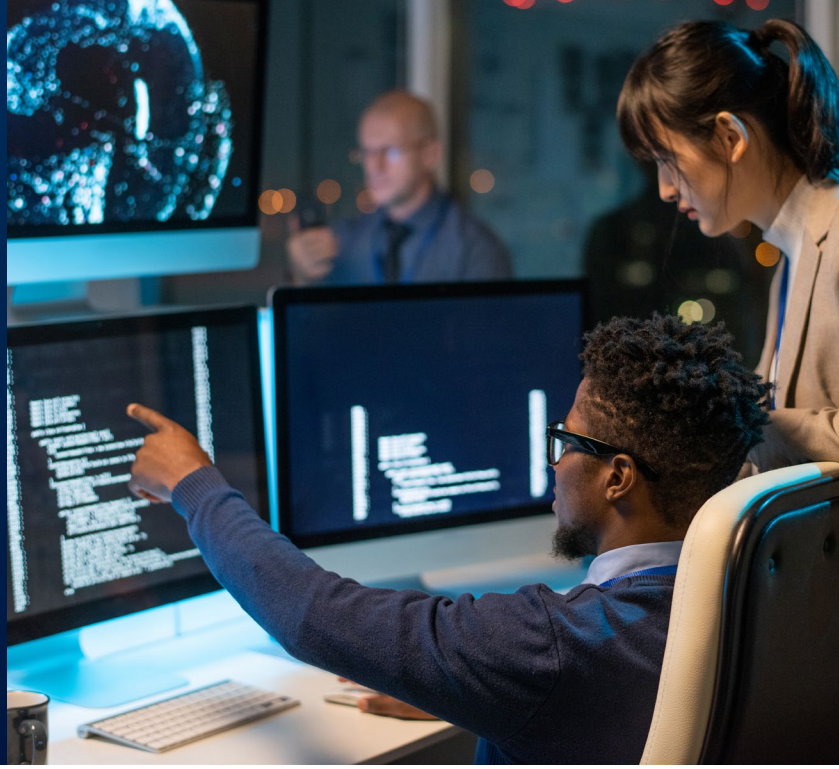
Brown & Brown



PROPERTY & CASUALTY

CISOs in the SEC's Legal Crosshairs

Authored by, Miles Crawford and Britt Eilhardt

Recent U.S. Securities and Exchange Commission (SEC) actions have ignited concerns that the scope of liability related to commercial data breaches now applies to individual members of targeted companies. The SEC's issuance of Wells Notices to the Chief Information Security Officer (CISO) and Chief Financial Officer (CFO) of SolarWinds marks a shift in tactics for the agency taking direct investigation into a company's handling of cybersecurity and response to an incident.

Previous SEC notices and actions were generally directed to companies rather than individual employees. Beyond the immediate legal implications, this development is reverberating with executives and cybersecurity professionals concerned by the potential for litigation and risk managers who may need to adapt their approach towards directors and officers coverage and cyber risk controls.

What is a Wells Notice?

A Wells Notice is a formal notice from the SEC informing a recipient that the agency plans to bring enforcement actions against them, likely regarding possible violations of securities laws. It is usually a formal letter or telephone call in which the staff enforcement attorneys of the SEC notify a target entity that they are planning to recommend enforcement action. While not indicative of any specific violation, the notice provides the potential target of a proposed enforcement action of the commission's plans and provides for a response.[1]

What Exactly Happened at SolarWinds?

SolarWinds, known for its Orion network monitoring platform, was under immense scrutiny after a 2020 cyberattack impacted its digital infrastructure, disseminated malicious updates and compromised customer data. On June 23, 2023, SolarWinds released a legal response, publicly revealing that they had received an SEC Wells notice on October 28, 2022. The SEC alleged a breach of duty on the part of SolarWinds directors, among other claims related to SolarWinds' cybersecurity disclosures and public statements, internal controls and disclosure controls.[2]

[1] SEC.GOV | INVESTOR BULLETIN: SEC INVESTIGATIONS. (2014, OCTOBER 22). https://www.sec.gov/oiea/investor-alerts-bulletins/ib_investigations

[2] UNITED STATES SECURITIES AND EXCHANGE COMMISSION, FORM 8-K 0001739942-23-000079 (d18rn0p25nwr6d.cloudfront.net)

The SolarWinds Wells notice follows earlier prosecution of Uber's Chief Security Officer (CSO), who, in October 2022, was found guilty of obstruction of proceedings and commission of a felony related to the 2016 Uber hack. The 2016 Uber hack resulted in massive numbers of sensitive records being compromised. Data belonging to approximately 57 million Uber users and 600,000 driver license numbers was stolen by hackers. Uber's CSO was sentenced to serve a three-year term of probation and ordered to pay a fine of $50,000 for his role in attempting to cover up the hack and obstructing the Federal Trade Commission's (FTC) investigation. The CSO's sentence sparked vigorous debate and attention from within the cybersecurity community over the potential personal liability of an individual executive.

A Paradigm Shift: CISOs in the Legal Crosshairs

What distinguishes these cases is the inclusion of the CISO in the Wells Notices and cybersecurity as a cause for SEC prosecution. Traditionally, Wells Notices have primarily targeted CEOs or CFOs in matters unrelated to cybersecurity. However, the SEC's decision to encompass the CISO signifies a pivotal shift towards holding cybersecurity professionals individually accountable for their actions. This new landscape raises questions about the role and responsibilities of CISOs, especially concerning the timely disclosure of material information related to cybersecurity incidents. As cyber insurance policies typically include coverage for privacy violations and data breaches, the SEC's action may prompt organizations to review and reassess their cyber insurance, the regulatory coverage therein (and the breadth of that coverage), and the interplay of cyber and directors and officers coverage.

How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.

Brown & Brown

Find Your Solution at BBrown.com

Brown & Brown, Inc. and all its affiliates, do not provide legal, regulatory or tax guidance, or advice. If legal advice counsel or representation is needed, the services of a legal professional should be sought. The information in this document is intended to provide a general overview of the topics and services contained herein. Brown & Brown, Inc. and all its affiliates, make no representation or warranty as to the accuracy or completeness of the document and undertakes no obligation to update or revise the document based upon new information or future changes.

©2023 Brown & Brown. All rights reserved.