ANDERSON KILL
Cyber Insurance Alert

New Cyber Risks from Regulators and Insurance Companies

By Seán McCabe

Key points:

A Wells Notice sent to SolarWinds highlights new regulatory risk stemming from cyberattacks.

Pending SEC rules are poised to mandate new reporting responsibilities following a cyberattack.

A new Lloyd's coverage exclusion for state-sponsored cyberattacks poses further issues for policyholders.

It's not news that the scale and cost of cyberattacks has been escalating for many years. Recently, however, increased regulatory pressure has added a whole new dimension to cyber risk. As those risks have increased, moreover, cyber insurance companies have moved to give themselves additional arguments to contest coverage. It is incumbent on companies not only to do as much as reasonably possible to defend against cyberattack, but also to ensure that their efforts are likely to comply with new and imminent regulatory requirements imposed by the SEC and other federal and state agencies. Further, companies need to be on guard with respect to their insurance policy renewals or new purchases for new exclusionary language.

The notorious SolarWinds hack of 2020-2021 now illustrates not only the enormous destructive reach of some state-sponsored cyberattacks, but also heightened regulatory risk. SolarWinds is a Texas-based network management software company. Beginning in February 2020, hackers injected trojanized code into one of SolarWinds' Orion software updates. The hack was blamed on cyber criminals with the Russian Foreign Intelligence Service. Through computer hacking, a malicious file was included in SolarWinds' Orion software updates. The trojan code provided the hackers with a 'backdoor'

which allowed them to remotely access an infected computer. SolarWinds inadvertently sent the infected software update to its customers, including large companies and federal agencies. Bedlam ensued. For the first 90 days of 2021 alone, SolarWinds estimated that the cost of the hack was about $19 million, excluding the reputational damage and the billions of dollars which would be required in the years to come to clear all malicious software from customer computer systems.

Now an additional unforeseen consequence to the SolarWinds hack has emerged. In an unprecedented move, reported in SolarWinds' most recent **8-K**, the Securities and Exchange Commission (SEC) has sent SolarWinds a 'Wells Notice' indicating the agency's possible intent to bring charges against the com-

pany. A 'Wells Notice' is a communication from the SEC to a person involved in an investigation that (1) informs the person that a preliminary determination has been made to recommend that the commission file an action or institute a proceeding, (2) identifies the federal security law alleged to be violated and (3) provides notice that the person may make a submission to the Division and Commission concerning the recommendation. The violation charged is yet unknown, but speculation, as **reported** in *The Washington Post*, is that it may involve failure to disclose information. The fact that the Wells Notice went to SolarWinds' Chief Information Security Officer (CISO) sent shock waves through the cybersecurity community and indicates a new level of exposure for company officers responsible for cybersecurity.

While conduct that the SEC is investigating in the SolarWinds matter predates the most recent rounds of proposed cybersecurity rulemaking, the *The Washington Post* cites a takeaway posted by Equifax CISO Jamil Farshchi: "But *if* this is about disclosure, it shows the SEC isn't sitting around waiting for cyber regs to be issued…They're taking action today."

The referenced "cyber regs" will doubtless increase exposure. The SEC's pending **proposed rules** for public companies are intended "to better inform investors about a registrant's cybersecurity risk management, strategy and governance, and to provide timely notification of material cybersecurity incidents…to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies that are subject to the reporting requirements of the Exchange Act."

This recent development has spawned a wave of anxiety amongst cyber executives. Equally concerning is the response of one major cyber insurance provider, Lloyd's of London, to court decisions finding that legacy "war risk exclusions" do not exclude insurance coverage merely because a cyberattack is attributed to state agents. Most notably, in *Merck & Co., Inc. v. Ace American Insurance Company*, a New Jersey trial court held in January 2022, and an appeals court agreed in May (475 N.J. Super.420 (May 1, 2023), that *Merck's* all-risk property policy covered $1.4 billion in losses stemming from the NotPetya attack – notwithstanding that in this case too, the malware was held to have been deployed by the Russian federation. Ace sought to apply a war risk exclusion barring coverage for losses stemming from "hostile or warlike action…by any government…or by any agent of such government." The court, placing the burden of proving the exclusion's applicability on Ace, ruled that the insurance company did not demonstrate that the exclusion applied under the circumstances of the case. The court reasoned that the plain language of the exclusion did not include a cyberattack on a non-military company that provided accounting software for commercial purposes to non-military consumers, regardless of whether the attack was instigated by a private actor or a 'government or sovereign power'.

The trial court in *Merck* noted that cyberattacks have long been a well-recognized risk, and that Ace could have expressly excluded coverage for such attacks if it wanted to. In a **Market Bulletin** dated August 16, 2022, Lloyd's declared that "cyberattack risks involving state actors…have additional features that require consideration." Effective March 31, 2023 or on the renewal of each policy, the bulletin required all Lloyd's cyber policies to include an exclusion for losses arising

A Lloyd's bulletin "required all Lloyd's cyber policies to include an exclusion for losses arising from any state-backed cyberattack in addition to any war exclusion."

from any state-backed cyberattack in addition to any war exclusion. As per the bulletin, these exclusions purport to:

"1. exclude losses arising from a war (whether declared or not), where the policy does not have a separate war exclusion.

2. (subject to 3) exclude losses arising from state backed cyberattacks that (a) significantly impair the ability of a state to function or (b) that significantly impair the security capabilities of a state.

3. be clear as to whether cover excludes computer systems that are located outside any state which is affected in the manner outlined in 2(a) & (b) above, by the state backed cyberattack.

4. set out a robust basis by which the parties agree on how any state backed cyberattack will be attributed to one or more states.

5. ensure all key terms are clearly defined."

Moving forward, some insurance companies (like Lloyd's) will be looking to arm themselves with coverage defenses to limit payouts under cyber policies for large claims. In addition, it appears that government entities such as the SEC and New York's Department of Financial Services are moving forward with civil enforcements against executives of firms who have been the victims of cyber crime. A new battleground for policyholders will be whether new exclusions for state-sponsored cyberattacks, stand-alone or added to existing war risk exclusions, will be used to contest coverage for purportedly state sponsored cyberattack. From *Merck*, it is clear that the vast majority of war exclusions in the marketplace do not apply to non-conventional acts of war like cyberattacks. The trial court in *Merck* stated, in fact, that: "It is also self-evident, of course, that both parties to this contract are aware that cyberattacks of various forms, sometimes from private sources and sometimes from nation-states have become more common. Despite this, Insurers did nothing to change the language of the exemption to reasonably put this insured on notice that it intended to exclude cyberattacks." The court thus all but confirmed to the insurance companies that their current exclusions could not properly be invoked.

It seems a cruel irony that while the SEC might hold a U.S. company responsible for a cyberattack against it, an insurance company might profess that a foreign government is somehow responsible – and accordingly try to deny coverage. Given those realities, policyholders must be vigilant in purchasing quality cyber policies that will cover the risks to which the company is actually exposed – and avoid policies that are sub-standard and beget disputes.

SEÁN McCABE *is an attorney in the New York office of Anderson Kill and a member of the firm's White Collar Defense and Insurance Recovery groups. Seán has had a key role in trial preparation and legal research on federal criminal cases arising out of the Southern District of New York, including major white collar criminal cases, conspiracy, and RICO cases. He also represents policyholders in insurance coverage disputes.*
smccabe@andersonkill.com
(212) 278-1029

We are interested in your feedback on topics for future articles and seminars. Please email us.

About Anderson Kill

Anderson Kill practices law in the areas of Insurance Recovery, Commercial Litigation, Environmental Law, Wills, Trusts and Estates, Corporate and Securities, Antitrust, Banking and Lending, Bankruptcy and Restructuring, Real Estate and Construction, Foreign Investment Recovery, Public Law, Government Affairs, Employment and Labor Law, Captive Insurance, Intellectual Property, Corporate Tax, Hospitality, and Health Reform. Recognized nationwide by Chambers USA, and best-known for its work in insurance recovery, the firm represents policyholders only in insurance coverage disputes — with no ties to insurance companies and has no conflicts of interest. Clients include Fortune 1000 companies, small and medium-sized businesses, governmental entities, and nonprofits as well as personal estates. The firm has offices in New York, NY, Newark, NJ, Philadelphia, PA, Washington, D.C., Stamford, CT, Los Angeles, CA, Denver, CO, and Boston, MA.