Insurance Companies Move to Expand Scope of War Exclusions

by Dylan LaMorte and Joshua Gold

The cyber insurance product market is more expensive and tighter than ever. Cyberattacks nearly doubled year-over-year in 2021, according to NCC Group. Insurance companies responded: Cyber insurance policy premiums increased by 110% in the first quarter of 2022, according to the Marsh Global Insurance Market Index. Those increases have not dampened demand. Marc Schein, a Marsh risk management consultant, told Axios in September that clients are still purchasing cyber insurance plans despite increasing cost. As of the second quarter of 2022, Marsh reported that for the first time, more than 50% of its clients purchased cyber insurance.

Compounding the challenges for policyholders seeking adequate cyber cover, Lloyd's is now attempting to broaden the scope of the traditional war exclusion as it pertains to cyberattacks. In Bulletin Y5381, released on August 16, 2022, Lloyd's set out requirements that standalone cyber policies include "a suitable clause excluding liability for losses arising from any state backed cyber-attack" in addition to any war exclusion already included in the applicable policy.

The bulletin states that at a minimum, the state-backed cyber exclusion must 1) exclude losses arising from war (whether declared or not), where the policy does not have a separate war exclusion; 2) exclude losses arising from state backed cyberattacks that significantly impair the ability of a state to function or that significantly impair the security capability of a state; and 3) clearly include or exclude coverage for computer systems located outside any state affected by the cyberattack.

It is no surprise that Lloyd's is responding to the recent surge in attacks from cybercriminal gangs affiliated, loosely or otherwise, with nation states and with the recent invasion of Ukraine by Russia. Thousands of companies have been displaced by the invasion, making companies throughout the world vulnerable to cyberattacks. But that does not mean that every cyberattack related to Russia is state-sponsored or an act of war.

Lloyd's is also doubtless responding to case law that has narrowed application of the war exclusion in the context of losses caused by terrorism. Under property insurance policies, courts have mainly deemed the war exclusion to have a narrow application to more conventional notions for military force and armed conflict between sovereign states. Courts typically will analyze certain factors when deciding whether a war exclusion would apply, such as 1) what type of physical weapons were used; 2) whether the actors were wearing military uniforms; and 3) whether any post war medals were awarded.

The reaction of Lloyd's to these decisions appears to be to add exclusionary language to the policies they sell. More specifically, the new Lloyd's exclusions respond to court decisions that have explicitly ruled the war exclusion inapplicable to cyberattacks that are alleged to have had state support.

For example, in a December 2021 decision *Merck & Co., Inc. v. Ace American Ins. Co.*, a New Jersey Superior Court ruled on summary judgment that a war exclusion did not apply to Merck's claim against its insurance companies for $1.4 billion in losses related to a NotPetya malware attack on 40,000 Merck computers. Merck purchased an all-risk policy with $1.75 billion in limits to cover losses or damages resulting from destruction or corruption

RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com

of computer data and software. The insurance companies argued that there was no coverage given the source of the malware, which the insurance companies argued "was an instrument of the Russian Federation" as part of its ongoing hostilities against Ukraine. Merck argued that the attack was a form of ransomware, rather than an official state action, and even if it was instigated by Russia to harm Ukraine, the war exclusion would not apply because the attack did not fall under the traditional forms of warfare as construed for insurance purposes.

The court emphasized that "the burden of proof is on the [insurance company] to show that a policy exclusion applies" and agreed with Merck's position that "no court has applied a war (or hostile acts) exclusion to anything remotely close to the facts herein." The court explained that the language used in war exclusions has remained "virtually the same for many years" and despite both parties being aware of cyberattacks, the insurance companies have "done nothing to change the language of the exemption to reasonably put [Merck] on notice that it intended to exclude cyber-attacks." The court granted summary judgment in favor of the policyholder that the war exclusion was not applicable.

The Merck court made clear that the war exclusion applied only to traditional forms of warfare, unless expressly agreed to otherwise. Lloyd's is now trying to potentially broaden the application of the war exclusion to exclude allegedly state backed cyberattacks. Bulletin Y5381 emphasizes repeatedly that the new provision excluding coverage for state-backed cyberattacks uses "robust wordings" to leave no doubt that "non-war, state backed cyberattacks" are not covered. The exclusion must "set out a robust basis by which the parties agree on how any state backed cyberattack will be attributed to one or more states" and "ensure all key terms are clearly defined." In sum, Lloyd's is attempting to redefine the historically narrow application of the war exclusion for cyber liability and cyber property damage policies by expanding it to exclude claims arising from state-sponsored cyberattacks.

The new Lloyd's exclusion could have ripple effects throughout the insurance industry. As such, policyholders should work with their insurance brokers to obtain the most favorable terms available in the insurance market. Policyholders should not solely focus on standalone cyber insurance products when they face losses or claims, to the exclusion of other avenues of potentially applicable coverage. They also may need to test insurance company positions as to the application and scope of these new exclusions. R

Dylan LaMorte is an attorney in Anderson Kill's Philadelphia office and a member of the firm's insurance recovery group. **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*, forthcoming from the Practicing Law Institute.

RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com