SOCIUS

New War and Cyber War Exclusions Take Effect

War exclusions are common in insurance policies. However, as the nature of warfare evolves, the insurance implications surrounding these exclusions become more complicated. One question is whether state-sponsored cyberattacks constitute acts of war. This concern is even more pressing in light of new requirements for cyber war exclusions from Lloyd's of London.

Traditional War Exclusions

According to IRMI, war exclusion provisions are present in nearly all insurance policies. These provisions exclude losses arising out of war or warlike actions. The war in question may be declared or undeclared, but it must be related to the use of military force under the direction of a sovereign power.

This raises a question: are cyberattacks an act of war?

State-sponsored cyberattacks are a known threat. For example, the Cybersecurity & Infrastructure Security Agency (CISA) issued warnings about North Korean state-sponsored cyber actors using Maui ransomware to target the healthcare sector and of Russian state-sponsored threats to critical infrastructure. The Department of Justice announced that a programmer backed by the North Korean regime was charged with conspiracy to conduct multiple cyberattacks and intrusions in connection to the WannaCry 2.0 ransomware attacks, which infected hundreds of thousands of computers globally.

Whether state-sponsored attacks like these constitute an act of war has led to debate. According to Reuters, U.S. Senator Dick Durbin called a suspected Russian hack of U.S. government agencies "virtually a declaration of war." However, legal and cybersecurity experts consider the hack to be an act of espionage rather than war.

What about attacks that seek to damage infrastructure rather than steal information? When it comes to insurance coverage, this gray area can complicate coverage. For example, according to Financial Times, some insurers argued that the NotPetya ransomware attack was a warlike action and the losses should not be covered.

SOCIUS

The Lloyd's Cyber War Exclusion Requirement

A new requirement from Lloyd's of London took effect on March 31, 2023.

According to the Bulletin from Lloyd's, "underwriters need to take account of the possibility that state backed attacks may occur outside of a war involving physical force. The damage that these attacks can cause and their ability to spread creates a similar systemic risk to insurers." Lloyd's says it is it's therefore important to use robust policy wordings.

Under the new requirement, all standalone cyberattack policies falling within risk codes CY and CZ must include a suitable clause that excludes liability for losses arising from state-backed cyberattacks, unless otherwise agreed by Lloyd's. In addition to excluding losses from declared and undeclared wars, the terms must exclude losses arising from state-backed cyberattacks that significantly impair the ability of a state to function or impair the security capabilities of a state.

Concerns Over the New Requirements

The new cyber war exclusion requirements have led to some concerns and pushback. According to Financial Times, people worry the exclusion will discourage companies from buying cyber insurance.
Another critical concern is it may not immediately be clear who is the perpetrator of an attack. If an insurer covers a ransomware event but later learns the attack was state-sponsored, what does this mean for coverage?

Cyber insurers may be unable to confirm whether an attack is backed by a state at the time of the attack, but policyholders will still need immediate resources. The immediate focus needs to be on removing the threat.

Many cyber policies include a hotline the policyholder can call after discovering a cyber incident. This essential feature of a rapid response can mitigate losses. Insurers invest significant funds into operating these hotlines. If a policyholder uses a hotline and the attack in question is later determined to be an act of war, will the policyholder need to reimburse the insurer for the costs incurred? It's important to ask questions like this, given the ambiguous nature of many cyberattacks.

The new Lloyd's requirement has only recently gone into effect. Only time will tell how it plays out.

The Gray Area of Cyber Warfare

As cyber losses have mounted, insurers have raised rates, increased underwriting requirements, and reduced the amount of coverage available. Now that Lloyd's has introduced new cyber war exclusion requirements, it is it's possible other insurers will follow suit. Securing robust cyber coverage was already difficult; going forward, it may be even more challenging.

Brett Klein
Assistant Vice President
Cyber, Professional, Management Liability Producer
email: bklein@sociusinsurance.com
mobile: (203) 830-9442