Published on *The National Law Review* https://natlawreview.com

Will an Act of War Destroy Your Cyberinsurance Coverage?

Article By:

Theodore F. Claypoole

Cyberinsurance spurs many complaints from US business. The cost is skyrocketing, retentions (deductibles) are rising quickly, and the insurance companies push their own panel lawyers on customers despite other relationships. Ransomware or email fraud can be excluded from some policies.

But news of significant hacks drives more companies into the cyberinsurance market despite the costs. According to Bloomberg, cyberinsurance prices rose nearly 100% in 2021 and keep climbing. Travelers Insurance, working to justify the leaping costs of its products, lists the following reasons for higher cybersecurity prices: a wave of ransomware, rising breach response costs (from forensic and legal experts to ransom payments and regulatory fines), increasing tech complexity and budgets, inadequate cybersecurity hygiene (which is why better controls can now lead to lower insurance prices), lack of advance response plans, and business interruption expenses. Shutting down business operations may be a way for criminals to force ransom payments, but it also creates an expensive risk reduction system, and all companies are suffering from it.

However, for the price of protection, you would expect your insurance company to pay to remediate a properly-reported cyberattack. Property insurers have long excluded “acts of war” from insurable damage that would receive payments. Most cyberinsurance policies have similar exclusions. This leads insurance customers to wonder, in a world where hackers and ransomware gangs from Russia and Ukraine initiate a significant percentage of cyberattacks, when would those attacks be considered “acts of war” during a real shooting war? If your company is smacked with ransomware from a Russian crew associated with the Kremlin, will your insurance company exclude the costs from your cyberinsurance policy as an act of war?

Lloyds of London just released a set of new exclusion clauses for addressing cyber war. These clauses are for underwriters to consider placing in Lloyds insurance contracts, and “have been drafted to provide Lloyd’s syndicates and their (re)insureds (and brokers) with options in respect of the level of cover provided for cyber operations between states which are not excluded by the definition of war, cyber war or cyber operations which have a major detrimental impact on a state.” Lloyds specifies that the “act of war” exemption language applies to China, France, Japan, Russia, the U.K and the U.S. The new clauses supply underwriters with extensive leeway to refuse to pay claims.Importantly, Lloyds can decide that the attack was an act of war even if the attackers do not declare themselves. Pending any government attribution of an attacker, Lloyds can decide through reasonable inference to attribute any attack to state activities, and therefor falling within the “act of

war” exclusion.

> Property insurers have long excluded “acts of war” from insurable damage that would receive payments. Most cyberinsurance policies have similar exclusions. This leads insurance customers to wonder, in a world where hackers and ransomware gangs from Russia and Ukraine initiate a significant percentage of cyberattacks, when would those attacks be considered “acts of war” during a real shooting war? If your company is smacked with ransomware from a Russian crew associated with the Kremlin, will your insurance company exclude the costs from your cyberinsurance policy as an act of war?
>
> TED CLAYPOOLE

All hope is not lost for businesses relying on cyberinsurance. Courts tend to hold insurers to high standards when trying to avoid paying out claims due to broadly-defined exclusions. For example, earlier this year the Superior Court of New Jersey rules that insurers can’t use a nation-state “act of war” cyber-exclusion to avoid covering more than a billion dollars in damages that Merck claimed it suffered from the NotPetya cyberattack in 2017. According to Insurance Journal, “ The insurers had tried to use the exclusions to avoid paying out, citing the fact the NotPetya malware was attributed to Russia and was meant to be deployed to disrupt and destabilize Ukraine. The malware wound up affecting thousands of companies worldwide. . . The cyber attack also attracted the attention of regulatory scrutiny of so-called “silent cyber” exposure in all policies.” The court “unhesitatingly” ruled that war exclusions did not apply in this instance.

So an attack from Russian hackers in 2021 may be covered under most cyberinsurance policies, but what about an attack in March of 2022? Does the state of hostility between the U.S. and Russian – in which Putin has claimed that sanctions against Russia and providing arms to Ukraine is an act of war – mean that ransomware attacks from the same Russian hackers may be considered acts of war? For example, the Conti ransomware gang has officially announced its full support of the Russian government after the invasion of Ukraine and threatened to use all possible researches to attack both Ukraine and Western countries that might support Ukraine. It would be easy for US critical infrastructure businesses to be direct victims of attacks from Russians supporting the Kremlin, or to be indirect victims of attacks aimed at Ukraine that spread through open networks like NotPetya or other malicious viruses. Where would that leave an affected company if its insurance provider refuses to pay, claiming an “act of war” exclusion?

We simply don’t know many insurance companies will use these policy exclusions and will be allowed to do so by U.S. courts. But each of us should check our cyber insurance policies for exclusions that could be triggered by current international conflicts.

Beyond insurance, international cyberattacks have straddled the line between standard crime and acts of international state hostility. Since the internet connected our world electronically, our societies have not set rules about how public and private actors are allowed to behave toward each other. Brad Smith, the President of Microsoft, has called for a Digital Geneva Convention, so that the nations of the world can agree what acts of electronic aggression are acceptable in war and even which acts should be considered to be acts of war. Maybe the current crisis, where a long-existing state is invaded without provocation, may be the catalyst to discuss digital hostility and set some rules around what kinds of interactions will be tolerated by the international community.

For now, check your cyberinsurance policies. For posterity, push our politicians to create baseline rules for the digital world. We have promulgated the law of the sea and the law of space. We should create a law of cyberspace as well.

National Law Review, Volume XII, Number 82