PAUL HASTINGS

Stay Current

February 2022

Follow @Paul_Hastings

Cyber War: How the Insurance Industry is Trying to Limit Cyber Coverage for Data Breaches

By Aaron Charfoos & Thomas L. Darby

Cybersecurity attacks are on the rise and companies are increasingly relying on their cyber insurance policies. At the same time, several carriers are looking to change the cyber insurance landscape to try to reduce their own exposure. A recent announcement from Lloyd's of London, and the responses of other insurance companies following the NotPetya ransomware attack, demonstrate that cyber insurers are trying to limit their coverage of these incidents. Given these competing changes, now is the time for companies to revisit their cyber insurance policies and how they respond to incidents.

Lloyd's and Cyber War

Lloyd's of London provided guidance in July 2020 that, except in very limited circumstances, its insurance policies will no longer cover costs stemming from war.[1] Then, in November 2021, the Lloyd's Market Association Bulletin published four "Cyber War and Cyber Operation Exclusion Clauses" providing additional interpretation of the July 2020 guidance to exclude all losses caused by "cyber war."[2]

Importantly, three of the exclusion options extend even further to cyber operations that are not simply "cyber war," but if they have a "major detrimental impact" on the functioning, security, or defense of a state.[3] This vague exclusion adds an extra wrinkle to an already murky world of cyberattacks by Advanced Persistent Threat (APT) groups who are often associated with countries and their militaries. In addition, while it has always been difficult to attribute a cyberattack to a specific APT or country, Lloyd's change appears designed to include all cyberattacks that target critical infrastructure regardless of the culprit. Under Lloyd's interpretation, a "cyber war" is defined by both the attacker or the victim. This change is likely to be challenged in court and the outcome of future cases will help shape our understanding of these policies.

Not Cyberwar

Lloyd's was not the first company to try to exclude cyberattacks under a war exclusion. Zurich American Insurance Company refused to pay a $100 million claim by Mondelez related to the 2017 NotPetya ransomware attack. Zurich claimed that the attack was "a hostile or warlike action in time of peace and war," based on official government statements from the U.S., U.K., Canada, and Australia, each of which attributed the attack to the Russian conflict with Ukraine. In the resulting lawsuit, Mondelez claimed that the Zurich insurance policy covers "all risk of physical loss or damage to electronic data, programs or software" as a result of "the malicious introduction of a machine code or instruction."[4] Given that

NotPetya was a ransomware attack consisting of malicious code, Mondelez filed a typical claim with Zurich for $100 million in damages from the attack. Zurich denied this ransomware claim based on a war exclusion. This lawsuit is in currently in the discovery phase.

A similar dispute involving Merck may provide instruction to insured companies on what is, and is not, going to be covered. Merck also reportedly suffered more than $1.4 billion in damages following the NotPetya attack. When Merck's insurance companies refused to cover these losses based on war exclusions, Merck filed suit for breach of contract.[5] This month, State Superior Court Judge Thomas J. Walsh found that Merck's insurance companies could not use a war exclusion to exclude cyberattacks.[6] Judge Walsh ruled that the insurance companies in question must update the language of their war exclusions to "reasonably put the insured on notice that it intended to exclude cyber attacks." In other words, insurance companies could only successfully evade covering cyberattacks if they had previously updated their policy terms to specifically exclude cyberattacks.

What Should Companies Do Now?

In light of this shifting coverage, is there anything companies can do now? Yes! Here are several steps you can take now to make sure your company is prepared for these changes in the marketplace of cyber insurance coverage:

- Review your existing policy to see what language is included in the war exceptions;
- Check to see whether your insurer has issued any guidance around these exclusions;
- Clearly understand any changes to policy terms during ongoing or upcoming negotiations; and
- If you do suffer an incident, be aware of whether any APT and other actors have been identified as the culprits (and the degree of certainty around that determination).

The Paul Hastings Data Privacy and Cybersecurity Group has significant experience providing counsel on insurance coverage for cyber incidents, responding to suspected security breaches and personal data disclosures, disputes with insurance carriers and guiding clients through investigations by federal authorities or class action lawsuits. If you have any questions concerning these developing issues, please do not hesitate to contact members of this team.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact the following Paul Hastings Chicago lawyer:

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

[1] *Performance Management—Supplemental Requirements & Guidance*, LLOYD'S OF LONDON (July 2020), https://assets.lloyds.com/assets/performance-management-supplemental-requirements-and-guidance-july-2020highlighted/1/Performance%20Management%20Supplemental%20Requirements%20and%20Guidance%20July%202020Highlighted.pdf.

[2] *Cyber War and Cyber Operation Exclusion Clauses*, LLOYD'S MARKET ASSOCIATION BULLETIN (Nov. 25, 2021), https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx.

[3] *Id.*

[4] Complaint at 2, *Mondelez international, Inc. v. Zurich American Insurance Company* (Ill.Cir.Ct. 2018) (No. 2018L011008).

[5] *Merck & Co., Inc., and International Indemnity, Ltd. v. Ace American Insurance Company*, Docket No. UNN-L-2682-18 (2021).

[6] *Id.*