LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Insurance Counseling & Recovery Practice May 23, 2023 | Number 3104

War Exclusion Developments in Cyber Insurance Policies

Policyholders have options when it comes to war exclusions in cyber insurance policies, a focus area for insurers following recent cyberattacks.

Key Points:

- Insurers have asserted that war exclusions may preclude losses arising from cybersecurity incidents outside the United States that result in a major detrimental impact to operations in the United States.
- Certain London Market insurers have promulgated recent guidance and revised model war exclusion clauses that they contend narrow coverage, which will be required in their cyber policies moving forward.
- Policyholders may be able to negotiate the terms of the war exclusion, place coverage with cyber insurers that are not modifying the language of the standard war exclusion, or find alternative insurance products with more favorable terms.

Businesses in the United States are increasingly the target of cyberattacks as advances in technology and tensions among governments continue to develop. When cyberattacks occur, it can be difficult (if not impossible) to identify the attackers and determine whether they are backed by a government. But the identity of the attacker can be a factor in whether the victim business is covered under its cyber insurance policy for the losses it suffers from the cyberattack, depending on the language used in the policy's so-called "war exclusion." In comparing and purchasing cyber insurance offerings, policyholders should carefully review the competing policies' war exclusions (advisably with the help of their broker and/or legal counsel), and be aware that there may be room to negotiate the terms of this exclusion or find alternative insurance products with more favorable language in the market.

Merck confirms appropriate scope and interpretation of war exclusions

Historically, war exclusions in first-party property and cyber insurance policies have been limited to cyberattacks that arise out of or are attributable to a "declared war" by a government. Today, in response to the rising number of sophisticated cyberattacks each year — including events that impact the availability of cloud or infrastructure services — some insurers have begun to advance the war exclusion beyond its traditional underpinning and in circumstances that do not involve military action. In a game-changing cyberattack in 2017 referred to as "NotPetya," malware linked to the Russian government caused damage around the globe and led to US$3 billion in insurance claims, some of which insurers contended were excluded.

To date, the courts have not agreed with insurers' arguments to expand the application of the war exclusion. In the most recent example, a New Jersey appellate court affirmed a lower court's decision that a war exclusion in property insurance policies issued to Merck & Co. Inc. (Merck) did not bar US$1.4 billion in coverage for losses stemming from the NotPetya attack.[1] Specifically, the property policies included a war exclusion that precluded coverage for "[l]oss or damage caused by hostile or warlike action in time of peace or war, including action in hindering, combating, or defending against an actual, impending, or expected attack." As part of the NotPetya attack, a hacker gained access to the computer systems of a Ukrainian company that had developed accounting software used by Merck and infected Merck's computer and network systems through that accounting software.

While the insurers conceded that those actions might not be "warlike," they argued that the actions were "hostile" within the meaning of the war exclusion because the events were "adverse," "showing ill will or a desire to harm," "antagonistic," or "unfriendly." Indeed, the insurers argued that any action that "reflects ill will or a desire to harm by the actor" falls within the hostile/warlike action exclusion, as long as the actor was a government or sovereign power, which they contended would include the Russian Federation in the NotPetya attack. However, the court rejected that argument and held that the exclusion clearly and unambiguously did not apply because it required "the involvement of military action" and not merely "damages arising out of a government action motivated by ill will." In fact, the court found that long-standing precedents "demonstrate a long and common understanding that terms similar to 'hostile or warlike action' by a sovereign power are intended to relate to actions clearly connected to war or, at least, to a military action or objective."

London Market's proposed modifications to war exclusions

Developments like the NotPetya attack and the *Merck* court's interpretation of policy language are impacting the cyber insurance marketplace in real time. Some insurers are responding by trying to narrow coverage through modified exclusions. For example, the latest cyber offerings from certain London Market insurers have adopted broader or more specifically worded war exclusions that may apply regardless of whether a war is declared by a government, and/or that extend to losses resulting from downstream impacts of actions by a government.

For example, last year Lloyd's of London published a bulletin in which it details certain "requirements" for war exclusions that are to be included in any Lloyd's policy at the inception or renewal of the policy, beginning on March 31, 2023. Under such requirements, the war exclusion must, for example:

- exclude losses arising from a war (whether declared or not) where the policy does not have a separate war exclusion;
- be clear as to whether cover excludes computer systems that are located outside any state that is affected in the manner outlined above, by the state-backed cyberattack;
- exclude losses arising from state-backed cyberattacks that significantly impair either the ability of a state to function or the security capabilities of a state;
- 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.

Lloyd's also published Cyber War and Cyber Operation Clauses Updates, drafted by the Lloyd's Market Association (LMA) Cyber Business Panel, to meet the Lloyd's requirements. These model clauses include Forms LMA5564, LMA5565, LMA5566, and LMA5567.[2] Even among these model clauses, there are important variances. Some examples include:

- LMA5564 does not exclude losses "arising from a **cyber operation** that causes a **state** to become an **impacted state**" (the other forms define "impacted state" to include "the functioning of that **state** due to the availability, integrity or delivery of an **essential service** in that state, and/or the security or defence of that **state**"). At the same time, the form does not provide any exceptions to the exclusion.

- LMA5565 provides a carve-back to the exclusion for to-be-specified limits on losses that would otherwise fall within the exclusion.

- LMA5566, which appears to be the broadest form in terms of exclusionary language, excludes losses regarding "impacted states" and does not provide any exceptions to the exclusion.

- LMA5567 provides an exception to the exclusion, stating that the exclusion shall not apply to "the direct or indirect effect of a **cyber operation** on a **computer system** used by the insured or its third party service providers that is not physically located in an **impacted state** but is affected by a **cyber operation**."

With the industry's increasing focus on cyberattacks as potentially posing a systemic risk, insurers may begin including more specific war exclusions in their policies, following the Lloyd's example. Policyholders should be particularly attuned to war exclusions that might exclude losses arising from an attack outside the United States that results in a major detrimental impact to their operations in the United States. For example, if Russia were to attack a computer system in Ukraine resulting in damage to a policyholder's (or its third-party service providers') computer system located in the United States, an exclusion for losses incurred by an impacted state might exclude those losses. An exception for such circumstances can ensure that those losses are covered.

Impact on policyholders for placing or renewing cyber insurance

In purchasing a cyber insurance policy, businesses should carefully consider the language used in any war exclusion. Policyholders may be able to propose different terms based on their relationship with the insurer. Some insurers, including certain London Market insurers, will require proposed changes to comply with the Lloyd's requirements, while other insurers continue to write policies with war exclusions that may be more narrowly tailored than what those requirements might allow. In any event, policyholders should not simply accept the exclusionary language without considering its potential impacts and trying, where appropriate, to negotiate different language. Cyber insurance is an important corporate asset, and the precise scope of exclusions in the policy can be the difference in whether a catastrophic cyberattack is covered or not.

If you have questions about this Client Alert, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

John M. Wilson
john.wilson@lw.com
+1.858.523.5463
San Diego

Steven B. Lesan
steven.lesan@lw.com
+1.858.523.5453
San Diego

Michael Huggins
michael.huggins@lw.com
+1.858.509.8408
San Diego

You Might Also Be Interested In

Hong Kong Privacy Regulator Highlights Data Security Guidance as Cyberattacks Increase

NHTSA Updates Cybersecurity Best Practices for the Safety of New Vehicles

New Cyber Incident Reporting Requirements on the Horizon in the US

Endnotes

1 *See Merck & Co. v. Ace Am. Ins. Co.*, No. A-1879-21, 2023 WL 3160845, at *1 (N.J. Super. Ct. App. Div. May 1, 2023).

2 On January 20, 2023, Lloyd's published alternative variations (Version B) of each of these forms, which omit the "Attribution of a **cyber operation** to a **state**" provision that appears in the initial versions (Version A) giving Lloyd's discretion to determine whether a cyber operation is attributable to a state. Therefore, the Version B forms are more favorable to policyholders than the Version A forms. However, Lloyd's has also stated that the Version B forms (unlike the Version A forms) do not comply with the Lloyd's requirements in this regard and therefore must have prior agreement from Lloyd's to be used.