The State of the Insurance Market for Cyber Incidents — Important Developments from 2023 and Looking Ahead in 2024

Client Alerts

February 7, 2024
By: Jan Larson, Steven Tinetti

As businesses have increasingly recognized the importance of obtaining insurance coverage specific to cyber incidents, so too have insurers increasingly recognized the risks inherent in providing such coverage - particularly where those cyber incidents potentially may be connected to sovereign state and government actors. In 2023, the insurance market introduced significant, substantive modifications to their policies in an attempt to address such incidents. Policyholders are encouraged to take a fresh look at the state of the insurance market for cyber incidents in light of these modifications and to examine and raise questions as to the availability and adequacy of such coverage going forward.

In January 2023, "following market feedback," the Lloyd's Market Association led the way in the market in announcing new, so-called model cyber war and cyber operation clauses. These updates included the following modified clauses:

- **LMA5564A/B:** Coverage is purportedly excluded for loss that "directly or indirectly aris[es] from a **war**"[1] and/or "aris[es] from a **cyber operation**."[2]
- **LMA5565A/B:** Coverage is purportedly excluded for loss that "directly or indirectly aris[es] from a **war**" and/or "aris[es] from **a cyber operation** that is carried out as part of a **war**, or the immediate preparation for a **war**" and/or "aris[es] from a **cyber operation** that causes a **state** to become an **impacted state**," meaning that the incident had "a major detrimental impact" on the ability of the **state** to provide an **essential service**—*g.*, financial market infrastructure—or on "the security or defence of that **state**." However, LMA5565A/B permits coverage for other **cyber operations** that do not fall within the scope of the exclusion at specified limits (in other words, state-backed cyber incidents that are not part of a war and do not have a major detrimental impact on a state.) But if no amount is specified, "there shall be no coverage for any **cyber operation(s)**."[3]
- **LMA5566A/B:** Coverage is purportedly excluded under the same terms as LMA5565A/B, without the permitted additional coverage for other **cyber operations** that do not fall within the scope of the exclusion at specified limits.[4]
- **LMA5567A/B:** Coverage is purportedly excluded under the same terms as LMA5566A/B; however, the "**impacted state**" exclusion does not apply to the "direct or indirect effect of a **cyber operation** on a **computer system**" that is affected but not "physically located" in the **impacted state**.[5]

The difference between the "A" and "B" versions of each clause is that the "A" versions include an additional clause related to the attribution process applicable to cyber incidents that the "B" versions do not include. That attribution clause provides that: "Notwithstanding the insurer's burden of proof, which shall remain unchanged by this clause, in determining attribution of a cyber operation to a state, the insured and insurer will consider such objectively reasonable evidence that is available to them. This may include formal or official attribution by the government of the state in which the computer system affected by the cyber operation is physically located to another state or those acting at its direction or under its control."[6]

Inclusion of one of these updated model cyber war and cyber operation clauses is mandatory in policies purchased from Lloyd's, rather than voluntary. Revisions can be authorized only where any such revisions remain in compliance with Lloyd's Market Bulletin Y5381.[7] Compliance with Market Bulletin Y5381 requires, in relevant part, the inclusion of "a suitable clause excluding liability for losses arising from any state backed cyber-attack in accordance with the requirement set out below" and "must be in addition to any war exclusion (which can form part of the same clause or be separate to it)."[8] As set forth in Market Bulletin Y5381, a suitable clause (if not one of the four updated model cyber war and cyber operation clauses) must, at minimum:

1. Exclude losses arising from a war (whether declared or not), where the policy does not have a separate war exclusion.
2. (Subject to 3) exclude losses arising from state backed-cyber-attacks that (a) significantly impair the ability of a state to function or (b) that significantly impair the security capabilities of a state.
3. Be clear as to whether coverage excludes computer systems that are located outside any state which is affected in the manner outlined in 2(a) & (b) above, by the state backed cyber-attack.
4. Set out a robust basis by which the parties agree on how any state backed cyber-attack will be attributed to one or more states.
5. Ensure all key terms are clearly defined.[9]

Other insurers and brokers subsequently followed suit, introducing proposed modifications to these model cyber war and cyber operation clauses, or in some instances new clauses, in an attempt to address cyber incidents purportedly involving sovereign state and government actors as part of the

evolving dialogue in the insurance market. For example, Chubb, Beazley, and Marsh have each made submissions to the London Market for review for compliance with Market Bulletin Y5381:

- Chubb: Purports to exclude coverage for (among other things) any malicious computer acts by states or state-sponsored groups that result in a declaration of war, the "ordering of actions that constitute the use of force," or "is cited as the reason in a resolution or other formal action" by the UN Security Council authorizing force or sanctions against another state, or that results in the use of force by NATO or an equivalent alliance.[10]

- Beazley: Purports to exclude coverage for any loss arising from a "cyber war," which means "any harmful act, conducted using a Computer System . . . directed against one or more Computer System" committed by or at the direction of a sovereign state that is conducted as part of a war or causes a "major detrimental impact on" the ability of another state to provide essential services or on the security or defense of that state. Like LMA5567A/B, the exclusion does not apply where an affected computer system is not physically located in the affected sovereign state.[11]

- Marsh: Purports to exclude coverage for any loss resulting from a war, a cyber operation carried out as part of a war, or a cyber operation that causes an "Impacted State," which refers to a sovereign state in which a cyber operation has had a major detrimental impact on the ability of that state to provide essential services or on the security or defense of that state. Like LMA5567A/B and Beazley's proposed exclusion, Marsh's proposed exclusion does not apply where the affected computer system is not physically located in the Impacted State.[12]

In light of the proliferation of cyber incidents and the potential high cost of the associated loss, insurers may be unwilling to insure against such risks, or certain categories of such risks, in the future—a potential outcome foreshadowed by the insurance market's recently introduced modifications to exclusions concerning cyber war and cyber operations involving sovereign state and government actors. As a consequence of these dynamic, changing conditions in the insurance market, looking ahead in 2024 and beyond, the obvious concern is that policyholders could be left without adequate and available coverage for potentially devastating cyber incidents that are alleged to involve sovereign state and government actors.

The insurance industry's apparent attempt to narrow and limit the coverage available to policyholders in the current insurance market, combined with the significance of potential market unavailability in the future, has led the insurance industry to advocate for a potential public, government-backed solution. Indeed, in discussing the impetus behind the Lloyd's updated model cyber war and cyber operation clauses, Lloyd's CFO stated that such exclusions were "needed to provide contractual certainty around *uninsurable losses*."[13]

In the aftermath of the September 11 terror attacks, Congress passed the Terrorism Risk Insurance Act ("TRIA").[14] The purpose of TRIA was to "establish a temporary Federal program that provides for a transparent system of shared public and private compensation for insured losses resulting from acts of terrorism" in order to protect consumers and allow for the private insurance market to stabilize.[15] TRIA was motivated by Congressional findings that the insurance industry was an important facet of the economy but may not have been able to adequately assess risk and insure against terrorist attacks.[16] Terrorism is arguably difficult to assess and predict, making it hard to insure against.[17] Additionally, losses from terrorism can be substantial and outpace any premiums that an insured might pay.[18] Indeed, as Congress noted, terrorist attacks can cause "widespread financial market uncertainties . . . including the absence of information from which financial institutions can make statistically valid estimates of the probability and cost of future terrorist events, and therefore the size, funding, and allocation of the risk of loss caused by such acts of terrorism."[19] Congress also recognized that the failure of the insurance industry to respond to such incidents could "suppress economic activity."[20]

Insurers may posit that the challenges in insuring against state-sponsored cyber incidents are arguably similar to those that Congress recognized in passing TRIA. Like terrorist attacks, cyber incidents are unpredictable, arguably making them more difficult to insure. Additionally, cyber incidents can cause potentially up to billions of dollars in losses,[21] making it difficult to efficiently price insurance premiums. As noted in Lloyd's Market Bulletin Y5381, "[i]f not managed properly [cyber related business] has the potential to expose the market to systemic risks that syndicates could struggle to manage … losses have the potential to greatly exceed what the insurance market is able to absorb."[22]

At the same time, there are significant obstacles to a federal backstop for cyber incident insurance. Cyber incidents are arguably more frequent than the type of attacks that would fall within TRIA (at least in the United States and Europe) and may become more frequent as states and their proxies develop increasingly sophisticated cyber warfare capabilities. Cyber incidents are also difficult to limit geographically—whereas terrorist incidents may pose risks to certain geographic areas, a cyber incident launched in one region could cause damage to a victim's computer systems across the globe. Consequently, it may be even more difficult (and expensive) to provide TRIA-like coverage for cyber incidents. Indeed, any such program likely would require significant funds (for example, through taxes) and may be politically unpopular to propose, particularly where the most likely beneficiaries of such a federal program would be companies and businesses making the largest claims.

The stakes are high as any inability of policyholders to recover losses caused by major cyber incidents could prevent policyholders from rebuilding or recovering after such incidents, potentially resulting in significant economic impact not only to those policyholders, but also to the broader economic ecosystems to which those policyholders contribute. In light of the recent activity around war and cyber operation clauses during the prior year, in 2024, policyholders are encouraged to continue to monitor the state of the insurance market and any action towards a public, government-backed solution and to seek the assistance of an insurance broker or counsel as needed for any concerns as to the adequacy or availability of cyber liability insurance coverage to fit their specific needs.

Footnotes

[1] Specially defined policy terms have been bolded for reference. A war is defined as an "armed conflict involving physical force" between two states whether war is declared or not. https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA23-003-PD.aspx. (LMA5564A, LMA5564B).

[2] A cyber operation is defined as "the use of a computer system by, at the direction of, or under the control of a state" to affect systems and information within that system. https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA23-003-PD.aspx. (LMA5564A, LMA5564B).

[3] *Id.* (LMA5565A, LMA5565B).

[4] *Id.* (LMA5566A, LMA5566B).

[5] *Id.* (LMA5567A, LMA5567B).

[6] *Id.* (LMA5564A, LMA5565A, LMA5566A, and LMA5567A).

[7] Lloyd's Market Bulletin Y5381,

[8] *Id.*

[9] *Id.*

[10] Cyber War Clauses, Lloyd's Market Association, https://www.lmalloyds.com/LMA/Underwriting/Non-Marine/Cyber_Clauses/cyber_war_clauses.aspx?WebsiteKey=6b59f78b-a7b1-4030-bd9a-63b40fe39ac4 (Cyber ERM General Amendatory Endorsement – Chubb).

[11] *Id.* (War and Cyber War Exclusion – Beazley).

[12] *Id.* (War and Cyber Operation Exclusion – Marsh).

[13] L.S. Howard, *Lloyd's Cyber War Exclusions: Confusing, Disruptive, but Necessary*? Insurance Journal (May 9, 2023), https://www.insurancejournal.com/news/international/2023/05/09/720020.htm#:~:text=Burkhard%20Keese%2C%20Lloyd%27s%20CFO%2C%20admitted,to%20accept%20that%20leadership%2C%E2

[14] Terrorism Risk Insurance Act, Pub. L. No.107-297, 116 Stat. 2322 (2002).

[15] *See id.* § 101(b).

[16] *See id.* § 101(a).

[17] *See* U.S. Gov't Accountability Off., GAO-17-62, Terrorism Risk Insurance: Market Challenges May Exist for Current Structure and Alternative Approaches 6 (2017)

[18] *See id.* at 1.

[19] *Supra* note 13, § 101(a)(4).

[20] *Id.*

[21] *See* Jonathan Berr, *"WannaCry" ransomware attack losses could reach $4 billion*, CBS News (May 16, 2017, 5:00 AM) https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/.

[22] *Supra* note 7.

Related Attorneys

Jan Larson
Partner
janlarson@jenner.com
+1 213 239 2273

Steven Tinetti
Associate
stinetti@jenner.com

+1 312 840 7360

Related Capabilities

Insurance Recovery and Counseling

Stay Informed →