Coverage for Cyber Attacks in a Time of War

Published by International Risk Management Institute.

COVERAGE FOR CYBER ATTACKS IN A TIME OF WAR

Sean Jordan, CPCU, MLIS, RPLU
Linda Robinson, CPCU, CRIS, ARM

March 2022

With the United States and much of the rest of the world imposing economic sanctions on Russia in response to its invasion of Ukraine, experts are warning of the possibility of retaliation by Russia in the form of cyber attacks. These attacks may be aimed at businesses as well as governmental entities. In this environment, it is important for businesses to understand how their insurance policies are likely to respond to losses caused by cyber attacks and what steps they can take to prevent or minimize losses.

Cyber-Attack Coverage under Commercial Property Policies

Generally, the extent of cyber-attack coverage provided by commercial property insurance policies depends on two things,

- whether the damage from the cyber attack is confined to electronic data or if other insured property is damaged and
- whether the policy contains an exclusion that may prevent coverage—typically, either a cyber exclusion or a terrorism exclusion.

Coverage for Damage to Electronic Data

A standard commercial property policy provides very little coverage for destruction or corruption of electronic data; the built-in amount is $2,500. More importantly for most organizations, a commercial property policy also provides very little coverage for business income or extra expense losses resulting from destruction, corruption, or other loss to electronic data. Once again, the built-in amount is $2,500. In the event of a denial-of-service attack, even these small coverage extensions may

not apply if the electronic data is not actually destroyed or corrupted.

Coverage for Damage to Other Property

The situation is different if a cyber attack causes direct physical damage from a covered cause of loss to covered property—such as the insured's computer equipment, machinery, or buildings. Suppose, for example, that hackers somehow gain control of the production machinery at a manufacturing plant and cause a fire or explosion at the plant. The damage from that fire or explosion would be covered under the commercial property policy—*unless a policy exclusion applies to prevent coverage.*

War Exclusion

The fact that Russia is waging war against Ukraine raises the question of whether the war exclusion in the insured's commercial property policy could apply to prevent coverage for damage due to a cyber attack that is known or suspected to have been directed by Russia in retaliation for the United States' support of Ukraine.

- The language of the war exclusion found in a standard commercial property policy clearly refers to what might be termed conventional warfare, and this interpretation has consistently been supported by the courts. One recent and very relevant case that upholds this interpretation is *Merck & Co., Inc., v. ACE Am. Ins. Co.,* No. UNN-L-002682-18 (N.J. Sup. Ct. Jan. 13, 2022). In this case, the court found that the insurer could not apply the war exclusion in the insured's commercial property policy to prevent coverage for loss to the insured's computer systems from the "NotPetya" malware, because its language is intended to apply only to traditional warfare and not to cyber attacks. Therefore, the war and military action exclusion *in a standard commercial property policy* should not apply to prevent coverage for damage from a cyber attack.

- However, commercial property policies written on *nonstandard forms* may contain war exclusions with language that specifically addresses certain types of cyber incidents as falling within the war exclusion. In these policies, the war exclusion alone may prevent coverage regardless of whether any other exclusion applies.

Cyber Exclusions

Most commercial property policies now contain a cyber-exclusion endorsement of some kind. For example, standard commercial property policies issued on forms drafted by Insurance Services Office, Inc. (ISO), must contain one of two cyber-incident endorsements.

- Both versions preserve coverage for resulting fire or explosion loss.
- The version that provides broader coverage does so by also preserving coverage for ensuing loss from other specific causes, subject to the limits of insurance shown in the endorsement schedule. The additional covered ensuing causes of loss vary depending on which of the causes of loss forms is included in the policy. However, none of the following is a covered ensuing cause of loss, regardless the attached causes of loss form: flood, radioactive contamination, breakdown, power outage, or molten material.

In the ISO cyber-incident exclusion endorsements, a cyber incident is defined as unauthorized access to or use of any computer system, including electronic data; a virus or other malicious or harmful code that is designed to alter, corrupt, disrupt, damage, etc., any computer system or its use or normal functioning; or a denial of service attack that disrupts, prevents, or restricts access to or use of any computer system or otherwise disrupts its normal functioning.

Cyber-attack exclusions that do not contain any exceptions (not even for ensuing fire) do exist and may be included in some nonstandard commercial property policies. A very broad exclusion of any and all loss resulting from a cyber attack could possibly prevent coverage of even a resulting fire loss.

Keep in mind that equipment breakdown loss is generally covered in a separate policy or under a separate coverage form within the commercial property policy. Therefore, it is also important to check the equipment breakdown policy or coverage section for a cyber exclusion that might prevent coverage for equipment breakdown caused by a cyber attack.

Terrorism Exclusions

If a cyber attack is deemed to be an act of terrorism, a terrorism exclusion or limitation in the policy could apply to prevent or limit coverage, even if the policy does not contain a cyber-loss exclusion. While standard commercial property forms do not exclude loss from terrorism, they can be endorsed to exclude coverage for loss due to terrorism or to limit it in some way in accordance with federal and state law. For example, suppose that hackers somehow gain control of the equipment at the power plant of an electric utility and cause a fire or explosion at the plant. Suppose further that it is learned that the cyber attack was carried out by terrorists and the event is declared by the government of the United States to be a "certified act of terrorism." If the utility company's commercial property policy contains an endorsement excluding

loss due to certified acts of terrorism, that endorsement would prevent coverage even if the policy does not contain a cyber exclusion.

Coverage under Cyber Insurance Policies

Insureds under cyber insurance policies should also be cautioned against expecting coverage for cyber attacks stemming from Russia's invasion of Ukraine and subsequent related incidents. While there is no "standard" wording used in the war exclusions found in cyber insurance policies, they are nearly always worded with the broad preamble of "based upon, arising out of, directly or indirectly involving, or in consequence of...." This wording excludes losses not only directly from warfare but also from attacks simply related to warfare.

Moreover, the breakout of physical, "kinetic" warfare in Ukraine gives the broadly worded war exclusions typically found in cyber insurance policies even more weight, compared to cyber incidents in the absence of any actual physical warfare. Recent litigation involving war exclusions like *Mondelez Int'l, Inc. v. Zurich Am. Ins. Co.* and the *Merck* case mentioned earlier (both involving the 2017 NotPetya attack) did not involve actual "boots on the ground" or physical warfare, leaving more room for courts to find coverage in favor of insureds (as they did in *Merck*). (Also, both of those situations involved more traditionally worded war exclusions in the insured's commercial property policies.)

This would likely not be the case for incidents stemming from Russia's invasion of Ukraine, which falls under the simplest definition of physical warfare found in relevant exclusions.

Nuances in War Exclusion Wording under Cyber Insurance Policies

While cyber insurance coverage should not be expected for attacks related to Russia's invasion of Ukraine, this development nevertheless provides an opportunity for insureds to review exactly how their policies' war exclusions are worded. Different phrasings can limit coverage even more so than other versions of exclusions, but there are also ways that insureds can slightly broaden their chances for future coverage related to nonphysical warfare.

In November 2021, a Lloyd's Market Association Bulletin released four draft war exclusions to act as a guideline for commercial

cyber insurers. We can draw out some of these wording nuances from those drafts.

- **Exclusion of both "war" *and* "cyber operations."** Insurers are taking steps to specifically exclude both these exposures when pertaining to one state taking action against another state. "War" definitions typically encompass more physical forms of warfare, while "cyber operations" will exclude uses of computer systems in a state-versus-state context. This has the effect of more explicitly broadening the scope of the war exclusion.

- **Attribution of an attack to a state.** Previous war exclusions on cyber insurance policies may have had an outright requirement that the attack must be attributed to a state. Now, per the Lloyd's bulletin, insurers may be shifting to attribution as a "primary but not exclusive factor." Again, this has the effect of broadening the exclusion to potentially bar coverage in more scenarios.

- **Operations by *or* on behalf of a state.** Another factor for insureds to be aware of is the exclusion of cyber operations not only *by* a state but also *on behalf of* a state. Attribution of a cyber attack to a state acting against another state on behalf of Russia, for example, would likely trigger a war exclusion in addition to cyber attacks coming directly from Russia.

- **Retaliatory operations between specified states.** Per the Lloyd's bulletin, one version of the draft war exclusions also specifically excludes coverage for "retaliatory cyber operations between any specified states," with "specified states" including a list of particular countries (China, France, Germany, Japan, Russia, United Kingdom, or United States are listed in the Lloyd's draft). This is yet another way that war exclusions are being explicitly broadened to bar coverage in more scenarios.

- **Detrimental impact on essential services.** Some war exclusions in cyber insurance policies may also specifically refer to a cyber operation that has a major detrimental impact on essential services in a sovereign state. In this case, an attack that disrupts financial institutions, health services, security and defense services, or utility services (just to name a few examples) would be excluded from coverage. With these types of institutions often being the first types of targets in a cyber-warfare environment, this is one more way of limiting coverage via the war exclusion.

- **Bystanding cyber assets carve-back.** One of the four Lloyd's draft exclusions contains an exception to the war exclusion that "carves back" coverage for "bystanding cyber assets," which are defined as computer systems used by either the insured

itself or its third-party providers that are not physically located in an impacted state but are nevertheless impacted by a cyber operation. This is favorable wording for an insured, but it should be noted that this exception in the draft exclusion *only* pertains to the "essential services" scenario described above.

- **Cyber-terrorism carve-back.** Finally, some cyber insurers' war exclusions also have an exception for "cyber terrorism." Cyber-terrorism attacks are usually defined as those intended to cause harm to or intimidate persons or entities, with the goal of achieving social, ideological, religious, or political objectives. The line between acts of cyber war and acts of cyber terrorism is blurry and can likely lead to claims disputes, but this exception is nevertheless favorable for insureds to have in a war exclusion.

In sum, war exclusions in cyber policies are broadening in scope, and draft exclusions such as the ones from Lloyd's are furthering that trend. Coverage for cyber attacks directly or indirectly stemming from Russia's invasion of Ukraine should not be expected under a cyber insurance policy, but insureds can take steps to at least make sure the phrasing of their war exclusions is optimized. An "ideal" war exclusion might do the following.

- Pertain only to "war," rather than to both "war" and "cyber operations"
- Require clear attribution to a state before coverage is barred
- Pertain only to actions *by* a state, rather than actions both by and on behalf of a state
- Be silent on retaliatory operations
- Be silent on detrimental impacts to essential services
- Contain an exception for cyber assets located outside the impacted state
- Contain an exception for acts of cyber terrorism

The ongoing hard market in cyber insurance may make these specific points difficult to negotiate, but insureds and their representatives should explore them. You can use *The Betterley Report* at the links on page 8 to compare how different insurers word their war-related exclusions in cyber-insurance policies.

Furthermore, insureds should be wary of critical cyber insurance underwriting factors like the following in order to secure the best coverage during hard market conditions.

- Network security measures
- Personnel, policies, and procedures
- Information security
- Website and content information
- Extent of contractual risk transfer
- Loss history

Cyber-Attack Risk Management

In the meantime, insureds can take the following steps to be proactive about protection against cyber attacks.

- Make cyber security a board-level issue
- Prevent cyber crime by utilizing security best practices, training, and the latest technology
- Secure and optimize cyber insurance coverage
- Have a plan for managing customer responses
- Engage a public relations firm ahead of time and have a plan following an incident
- Be prepared to send required notifications to affected parties
- Have a forensic investigation and system response plan
- Have a plan for a legal response and maintain a law enforcement contact
- Finance the response
- Have a response team organization chart
- Conduct tabletop exercises (a service that is often offered by cyber insurers) to work through cyber-attack scenarios

Links to More Information for Subscribers

IRMI subscribers can find more detailed information on these topics here.

Coverage and Exclusionary Wording

- Cyber-Attack Coverage under Commercial Property Policies (Vertafore Subscribers/ IRMI Online Subscribers)
- War And Military Action Exclusion in ISO Special Causes of Loss Form (Vertafore Subscribers/ IRMI Online Subscribers)
- Cyber Insurance War Exclusions (Vertafore Subscribers/ IRMI Online Subscribers)
- *The Betterley Report*—Cyber/Privacy Insurance Market Survey—2021 (Vertafore Subscribers/ IRMI Online Subscribers)

Risk Management and Loss Control

- Developing a Cyber Event Response Plan (Vertafore Subscribers/ IRMI Online Subscribers)
- Cyber and Privacy Loss Control (Vertafore Subscribers/ IRMI Online Subscribers)

Cyber Underwriting

- Cyber Insurance Underwriting Factors (Vertafore Subscribers/ IRMI Online Subscribers)

About IRMI®

For over 40 years, International Risk Management Institute, Inc. (IRMI), has been a premier provider of practical and unbiased risk management and insurance information to a subscriber family that now includes thousands of risk, insurance, and legal professionals serving all industries across the globe. IRMI also publishes an extensive library of free articles, white papers, a glossary, and other content on IRMI.com, one of the most visited websites for risk professionals. Our vast KnowledgeBase, available online through our own platform and as part of Vertafore's ReferenceConnect service, is developed by the most experienced research and editorial team in insurance reference publishing in partnership with a host of industry practitioners who work with us. We take great pride in giving you up-to-date, objective, and practical strategies, tactics, and solutions to help you succeed and prosper in a changing insurance and risk management environment. This content can be accessed through the insurance analyses, conferences, online continuing education courses, and industry-specific certifications we offer.

Secure Expertise. Secure Credibility. Secure Success.

Access Content
Attend a Conference
Obtain CE Credit
Earn a Certification
Sign Up for Free Risk and Insurance Email Newsletters

International Risk Management Institute, Inc.
12222 Merit Drive, Suite 1600 • Dallas, TX 75251 • (972) 960–7693 • www.IRMI.com