MARSH JLT SPECIALTY

"SILENT CYBER"

Frequently Asked Questions (and Answers)

NOVEMBER 2019

MARSH

MARSH JLT SPECIALTY

"SILENT CYBER"
FREQUENTLY ASKED QUESTIONS

This document provides Marsh's explanation of the concept of "silent cyber"; the changes that many insurers are making to exclude coverage of cyber perils from traditional non-cyber insurance policies; and our recommendations help clients adapt to these changes and ensure they have adequate protections against cyber losses.

Q: What is "silent cyber?"

A: "Silent cyber" or "non-affirmative" cyber refers to potential cyber exposures contained within traditional property and liability insurance policies which may not implicitly include or exclude cyber risk. Unlike specialist standalone cyber insurance, which clearly defines the parameters of cyber cover, traditional insurance policies were not designed with cyber exposures in mind. In many cases, traditional policies will not specifically refer to cyber and could theoretically pay claims for cyber losses in certain circumstances. This is particularly true for all-risk property coverages that do not exclude cyber risk – also known as "non-affirmative" cyber – and is also relevant for marine, aviation, transport, and property lines, as well as some liability covers.

Q: Is there a commonly understood definition for what "cyber" means in this context?

A: While the public focus is often on malicious attacks on computer systems that lead to losses, cyber risk does not need to have a malicious component, and indeed some cyber insurance wordings will also consider a broad range of technology failures as in-scope. The most commonly agreed definition of "cyber risk" is that which has been proposed by the UK Prudential Regulation Authority and endorsed by Lloyd's:

> *"Any risk where the losses are cyber-related, arising from either malicious acts (e.g. cyber-attack, infection of an IT system with malicious code) or non-malicious acts (e.g. loss of data, accidental acts or omissions) involving either tangible or intangible assets."*

Q: Isn't silent cyber a good thing for policyholders?

A: Not really. The lack of clarity in some standard property and casualty policies has led some companies to believe that they have adequate cover for cyber risk when they may not. Further, as cyber risk continues to evolve, non-affirmative language within a traditional insurance policy may be subject to differing interpretation by insurers, which could lead to disputes with policyholders that would require the intervention of the courts.

MARSH

MARSH JLT SPECIALTY

Q: Why are the insurers concerned about silent cyber?

A: Insurers and regulators are concerned that silent cyber can represent a significant unmeasurable and unexpected risk to insurers' portfolios. This can be especially significant if there is exposure to systemic risk. An insurer of a non-affirmative wording would not have considered the potential cyber risk that is inadvertently covered, and therefore would not have rated this hidden risk and calculated the increased exposure of the policyholder, or adjusted the premium accordingly.

Ambiguity in coverage may also be holding the insurance market back, according to Marsh research. For example, insurers are concerned that cyber exposures are contained in traditional policies by virtue of not being excluded, which raises the prospect of unexpected losses in the event of a cyber incident. This has created the situation where cover is often not properly provided or understood.

Q: What are the insurers doing to eliminate "silent cyber"?

A: Insurers are taking several steps to address silent cyber, some of which are required by regulators. Some insurers have made announcements that clarify their intent as regards coverage. These announcements are "patches" as insurers maneuver to introduce new policy language and underwriting guidelines. Other announcements, such as those issued by Lloyd's and some company market insurers, have also made clear that, effective a certain date, they will either expressly exclude or include cyber risk in their traditional lines policy wordings. The earliest effective date of these changes is January 1, 2020, which applies to coverage for first-party property damage policies underwritten by Lloyd's syndicates.

Q: What do these "silent cyber" exclusions do?

A: The silent cyber clarifications or exclusions vary by product and insurer. The typical language defines cyber risk and then excludes it from a particular policy. Some insurers have taken a more nuanced approach by including wording that would first provide affirmative cover for cyber risk, and then either grant the coverage with or without some limitations, such as sub-limits or zero out the limit as an effective exclusion.

Q: Am I losing coverage if my insurer adds a cyber exclusion to my policy?

A: Not necessarily, given that cover may not have been certain to begin with, as explained above. You need to carefully examine any exclusion, as several silent cyber exclusions may be overly broad for your needs. The goal of any exclusion should be to specifically exclude only that which an insurer is not expressly willing to cover and rate, and to do so with precision. Care needs to be taken to ensure that these exclusions do not overreach and unduly restrict the cover that you require.

MARSH JLT SPECIALTY

Cyber exclusions should not impact the core coverages offered in the product you are seeking. For example, here are two scenarios for policyholders to consider when reviewing and evaluating potential exclusions:

1. If a computer virus causes a piece of equipment to overheat, which leads to a fire that burns down the building – would you want the resulting fire loss to be covered in your property policy?

2. Should a cyber liability exclusion on a D&O policy remove coverage for a shareholder class action because the underlying allegation is that management mishandled a cyber event or failed to make the proper disclosure of such event when it crested a materiality threshold?

Q: What should I do if I want affirmative cyber coverage under my non-cyber policy?

A: Depending upon the insurance product and the insurer, you may be able to purchase affirmative cyber coverage under a non-cyber policy. Care should be taken, though, in how the insurer adds the coverage, as indicated in the scenarios provided in the previous answer. In addition, thought should be given to whether having affirmative cyber coverage in a non-cyber policy best serves your interests. In most cases, the cyber coverage available in a standalone cyber policy will be superior (both in terms of its breadth and limits) to what can be obtained by adding affirmative cyber coverage to a more traditional line of non-cyber insurance which is not designed to cater for cyber risk.

Q: If my non-cyber insurers insist on broad exclusions, is there a solution in the cyber market?

A: It's very likely that the standalone cyber market can offer a full or partial solution to fill many of the gaps that result from a silent cyber exclusion. You will need to provide the traditional policy's underwriting submission and additional cybersecurity underwriting information, and work with your broker to clearly articulate the loss scenario that sits in the gap. The key limitation of the cyber market is capacity: a maximum of $500 million to $750 million in limits is available depending on the breadth of coverage. There are many creative approaches to "silent cyber" and discussion with your broker will help identify how best to meet your needs.

Information and Contacts

For more information or questions about "silent cyber", please contact your local cyber team or:

Bob Parisi
Cyber Product Leader
Robert.Parisi@Marsh.com

Sarah Stephens
UK Cyber Practice Leader
Sarah.Stephens@Marsh.com

MARSH JLT SPECIALTY