MARSH JLT SPECIALTY

SEPTEMBER 2020

"Silent Cyber" — Frequently Asked Questions

Property and Casualty Insurance Concerns Resulting From Compliance With "Silent Cyber" Mandates

MARSH

The ubiquitous use of technology has transformed the business landscape, intensifying the likelihood of cyber losses and the scope and scale of cyber exposures for all organisations. From an insurance perspective, this has led to the rise of so-called “silent cyber” issues, or non-affirmative coverage for cyber risk in non-cyber policies.

As a result, new risk issues are emerging as insurers individually interpret and seek to comply with silent cyber mandates by adopting various exclusions, limitations, and changes to traditional non-cyber insurance policies.

Following are some frequently asked questions regarding silent cyber, along with our recommendations as to how organisations can address these changes and ensure they have adequate protection against cyber losses.

What is silent cyber?

As technology has come to define much of the modern business era, cyber-attacks have progressed beyond simple data breaches to sophisticated schemes designed to disrupt business operations and supply chains.

As a result, traditional lines insurers have expressed concern that claims stemming from cyber risks — risks that they had neither underwritten to nor charged for — are creating unmeasured exposure in their portfolios. In this context, we define cyber risk as the possibility of loss or injury relating to or involving data or technology. This phenomenon of non-affirmative coverage for cyber risk in non-cyber policies is known as silent cyber.

Silent cyber can arise in a number of ways, for example, if:

- Cyber events as triggers for loss are not explicitly included or excluded.
- Cyber exclusionary language within the policy is ambiguous or absent.
- Any express cyber coverage is ambiguous or conflicts with other policy wording.

Why is silent cyber an issue now?

For many years, regulators and global insurers have reviewed non-affirmative cyber risks and exposures within property and casualty (P&C) insurance portfolios. In the UK, the Prudential Regulation Authority (PRA) and Lloyd’s have driven the agenda on this issue. In January 2019, the PRA issued a letter to all UK insurers that stated they must have “action plans to reduce the unintended exposure that can be caused by non-affirmative cyber cover”. Also in 2019, Lloyd’s issued a market bulletin mandating that all policies must be clear on whether coverage is provided for losses caused by a cyber event, thereby eliminating silent cyber exposure. This was to be accomplished by either excluding from or affirmatively covering the exposure in all P&C policies. The deadline for this initial phase of the mandate, covering first-party property insurance, was 1 January 2020.

Further bolstering these mandates, rating agencies, such as Fitch, have cited failure to manage these exposures as ratings criteria. It is expected that the European Insurance and Occupational Pensions Authority will issue a similar message.

What are examples of silent cyber risks that are covered by traditional lines of insurance?

Silent cyber can arise as an issue in various insurance policies in a number of ways (see Figure 1).

	Policy type	Potential trigger
	PROPERTY Covers material damage and business interruption from physical loss or damage to tangible property.	Malware attack scrambles the data in a programmable controller, leading to a fire in a production facility.
	CASUALTY Third-party bodily injury and property damage liability in sectors such as marine, aviation, and automotive.	Software update to key operating systems has bad code, causing systems to go offline during operation, leading to crashes and causing the operators/owners to incur liability.
	GENERAL LIABILITY Third-party bodily injury, property damage liability, advertising, and personal injury.	Cyber-attack causes a store's heating system to overheat, causing an explosion. Bodily injury and property damage ensue.
	DIRECTORS & OFFICERS Coverage for litigation or regulatory action arising out of failure to disclose, misrepresentations, or breaches of fiduciary duty.	Publicly traded company experiences a data breach, ultimately leading to a stock price drop, and a securities class action lawsuit follows.

How are requirements from Lloyd's, the PRA, and others affecting traditional P&C insurance programmes?

The mandate and short timeline from Lloyd's has led most insurers to apply exclusions rather than to affirm cover, citing concerns over the potential aggregation risk from a systemic loss. To date, many of the proposed cyber endorsements on traditional P&C policies have been inconsistent, and in some cases overly broad, for example, excluding ensuing loss from previously covered physical perils simply because technology was involved somewhere in the chain of causation. Many proposed wordings by insurers still overlook or misunderstand the fact that technology is integral to business operations across all sectors.

Has Lloyd's issued a definitive list of approved clause wordings?

No. The Lloyd's market bulletins require insurers be clear in defining if there is (or is not) coverage for losses caused by a cyber event. There is no requirement to exclude cover and no requirement to limit or sublimit cover, only the requirement to be clear to clients on what cover exists. Various Lloyd's committees have published suggested endorsements, but Lloyd's has not mandated the use of any of them. Insurers are free to apply any wordings they feel comply with the requirements.

If there is no mandated exclusion of cover or defined list of clauses, what actions are insurers taking?

Insurers have various options for addressing silent cyber, including:

- Affirm all otherwise-covered resultant loss exposure within a policy, regardless of the involvement of technology.
- Affirm all otherwise-covered resultant loss exposure contained within the policy, but sub-limit the cover available.
- Exclude all otherwise-covered resultant loss exposure contained within the policy.
- Exclude all otherwise-covered resultant loss, but insert write-backs for certain perils/losses.

To date, insurers have favored the last two options, but often use vastly different language. In some cases, this variance has made the coverage less clear.

Insureds should work with their broker to understand the impact of any proposed wording changes on protections offered by their policies, and investigate all coverage options available, including alternative express cyber coverage options.

What are the options when presented with an endorsement modifying silent cyber on a P&C policy?

The varied approach from insurers, coupled with each organisation's unique risk profile, means that one solution will not fit all and that a number of options should be considered when evaluating coverage issues created by any new silent cyber clause (see Figure 2).

FIGURE 2

Insureds have a number of options to consider when facing cover changes resulting from proposed silent cyber exclusions.

Note: None of these options alleviate the need to purchase a standalone cyber policy for full scope of cyber coverage. A combination of options may be best, for example, requesting a less restrictive exclusion and purchasing a "gap filler" policy.

OPTION	ADVANTAGES	DISADVANTAGES
Reject the exclusion.	• Not paying for "phantom" residual loss cover. • Retain coverage for resultant physical cyber losses.	• Lloyd's insurers will not offer capacity without silent cyber wordings as that puts them out of compliance. • Likely to reduce the overall capacity available to you for risk transfer.
Request a less restrictive version.	• Better coverage certainty. • Retain coverage for some resultant physical perils, typically fire and explosion.	• Some resultant physical perils will still not be covered. • Typically won't include coverage for malicious cyber events.
Accept the exclusion as offered.	• Easiest path to retention of overall coverage capacity.	• Likely to exclude more resultant physical loss than expected. • May need to sue insurer for coverage following a carrier declination.
Accept the exclusion and purchase a "gap filler" policy.	• May improve overall coverage.	• Gap filler policies tend to be expensive. • Coverage offered may not fully replace coverage taken away by the cyber exclusion.

What approach does Marsh recommend for addressing silent cyber modifications to P&C programmes?

As organisations address silent cyber issues, they should look for solutions that aim to maximise coverage, restrict potential coverage gaps and overlaps, and maximise potential recoveries (see Figure 3).

FIGURE 3

In approaching silent cyber, look to limit gaps and overlaps and maximise coverage.

TRADITIONAL POLICIES

- Should cover resultant physical damage or bodily injury regardless of technology involvement.
- Should cover malicious and non-malicious acts.
- Should delineate between physical and non-physical impacts.
- Cyber events involving IT/OT/Comms:
  - Loss affirmed for physical damage.
  - Replacement or loss of computers can be excluded if covered by cyber policy.
  - Non-physical loss can be excluded if covered under cyber policy.

CYBER EXCLUSIONS

- Should not overreach to restrict or remove core policy cover simply because technology or data was impacted or implicated in the chain of causation.
- Should not conflate underlying intent of the bad actor with impact to the insured.
- Should be clear when delineating between physical and non-physical impact.

STANDALONE CYBER INSURANCE

- Provides coverage that is typically superior (limits and breadth) to adding affirmative cyber sublimits to non-cyber policies.
- Should cover losses arising from the confidentiality, integrity, or availability of data or technology.
- Typically provides US$500 million to US$700 million limit capacity.
- Should provide broad coverage for first- and third-party risks:
  - Incident response.
  - Business interruption (non physical).
  - Data breach.
  - Data restoration, hardware replacement.
  - Cyber extortion.

MARSH APPROACH TO SILENT CYBER

Marsh offers specific solutions and advice to help organisations address silent cyber. Our approach is twofold:

Short term: The changes insurers are making to address silent cyber mandates can create coverage gaps — even as new, emerging risks and technologies are increasing organisations' exposures and coverage requirements. We look for wording changes that potentially create gaps in existing insurance programmes. We seek to adapt and amend the best wordings and clauses available, advocating for these with underwriters.

Long term: We seek the adoption of clear, affirmative language that provides full policy coverage across traditional policies; for example, language that ensures property policies cover physical damage irrespective of the presence of technology in the causation of loss.

What about standalone cyber coverage? Can it address any gaps in cover?

Although there is some property damage capability and capacity available from cyber insurers, the best approach is to review your overall coverage requirements with your insurance adviser. There are innovative standalone cyber covers that may provide additional protection and benefit to your organisation (see Figure 4).

What additional developments are likely in 2020?

Marsh anticipates the following factors to develop or continue in the months ahead:

- No consistent approach by insurers across traditional lines regarding affirming/excluding/sub-limiting cover.
- A lack of consistency and relatively more limited market capacity among cyber product solutions, compared to new P&C exclusions, in accordance with exclusions introduced.
- A need to address the gaps in cover that may be created by exclusionary language/sublimits.
- Limitations in cover introduced by non-cyber insurers.

Assessment of non-affirmative exposures is a continuous cycle: new risks are continually being introduced to traditional lines as advances and use of technology accelerates.

FIGURE 4 Standalone cyber insurance policies offer broad coverage for financial risks, but limited physical damage coverage.

ELEMENTS OF CYBER RISK OFTEN COVERED BY CYBER POLICIES

- Incident response expense.
- Data breach liability.
- Non-damage business interruption.
- Data restoration expense.
- Liability for compromises of confidential information.
- Cyber extortion.
- Non-damage hardware replacement (bricking).
- Physical damage (where available, but has limited capacity. This is the gap that traditional markets must fill.)

CONSIDERATIONS FOR BUYERS

Buyers have traditionally found cover for physical loss or damage in non-cyber policies, such as property insurance (see Figure 3).

When seeking cover for physical loss or damage, buyers are advised to consider the following:

- Ease of placement/underwriting information.
- Approach to date.
- Pricing.
- Capacity.
- Competitiveness of London market.
- Other policies purchased that already address the risk.

We’re here to help you.

Marsh’s team of 230 specialised cyber risk management professionals works with clients in every market worldwide. We encourage you to reach out to them to help you stay up to date on the full scope of solutions available.

For more information or if you have additional questions about silent cyber, please contact your Marsh representative or the Marsh cyber team.

- Our Silent Cyber webpage will help keep you updated.
- The Marsh cyber team can be reached at cyber.risk@marsh.com.
- Or you can contact any of the members of our dedicated US Silent Cyber team:

CYBER

Elisabeth Case
elisabeth.case@marsh.com

Bob Parisi
robert.parisi@marsh.com

Tim Marlin
timothy.marlin@marsh.com

PROPERTY

John Hughes
john.f.hughes@marsh.com

Scott Patterson
scott.m.patterson@marsh.com

MARINE

Guy Claveloux
guy.p.claveloux@marsh.com

Paul Friel
paul.a.friel@marsh.com

Tom Deist
thomas.a.deist@marsh.com

Herman Brito
herman.brito@marsh.com

CASUALTY

Burt Garson
burt.m.garson@marsh.com

Jesse Paulson
jesse.paulson@marsh.com

FINPRO

Robert Salinardo (Bermuda)
robert.l.salinardo@marsh.com

Sarah Downey
sarah.d.downey@marsh.com

Barry Mansour
barry.mansour@marsh.com

MARSH'S CYBER INSURANCE PRACTICE BY THE NUMBERS

230
GLOBAL CYBER COLLEAGUES (BROKERS AND CONSULTANTS).

PLACING MORE THAN
$1 BILLION
PREMIUMS ANNUALLY.

MORE THAN
6,300
CYBER AND E&O CLIENTS.

LEADER OF
25 YEAR-OLD
CYBER INSURANCE MARKET.

BROKER TEAM OF THE YEAR ($500M+)
BUSINESS INSURANCE US AWARDS 2019.

CYBER BROKER OF THE YEAR
ADVISEN 3 TIME WINNER.