MARSH JLT SPECIALTY

AUGUST 2020 UPDATE

"Silent Cyber" — Frequently Asked Questions

Property & Casualty Insurance Concerns Resulting from Compliance with "Silent Cyber" Mandates

MARSH

In this update, we highlight some of the new risk issues that are emerging as insurers individually interpret and seek to comply with 'silent cyber' regulatory mandates by adopting various exclusions, limitations, and changes to traditional non-cyber insurance policies.

We also provide our recommendations to help Marsh clients and other organisations adapt to these changes and ensure they have adequate protections against cyber losses.

I have heard a lot about "silent cyber." What is it?

The advances and ubiquitous utilisation of technology in nearly all enterprise assets and operations has transformed the business landscape, while intensifying the likelihood, scope, and scale of cyber risks for all organisations. In this context, cyber risk is defined as the *possibility of loss or injury relating to or involving data or technology.* In parallel, cyber-attacks have progressed beyond simple data breaches to sophisticated schemes designed to disrupt businesses and supply chains.

As a result, traditional lines insurers have seen that claims stemming from cyber risks — risks that they had neither underwritten to nor charged for — are creating unmeasured exposure in their portfolios. 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:

- Cyber events as triggers for loss are not explicitly included or excluded;
- Cyber exclusionary language within the policy is ambiguous or absent; and/or
- 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 & 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 January 1, 2020.

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

Cyber Risks May be Covered Under Various Lines of Insurance
Examples of Silent Cyber Triggers in Non-Cyber Policies

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

Marine, aviation, automotive — third-party bodily injury and property damage.

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 drop** and a securities class action lawsuit follows.

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

Unfortunately, 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 for aggregation 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, to exclude 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:

- 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 favoured the last two options but often using vastly different language. In some cases, this variance has made the coverage even less clear than before.

Marsh recommends that our clients and other organisations work with your broker to understand exactly what impact any proposed wording changes may have on your protection 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. The following options should be considered when evaluating coverage issues created by any new silent cyber clause.

Buyer Options to Consider When Facing Proposed Cover Changes Resulting From Silent Cyber Exclusions

Note: None of these options alleviate the need to purchase a stand-alone 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 of London 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 of 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 provide better overall coverage.	• Gap filler policies tend to be expensive. • Coverage offered may not fully replace coverage taken away by the cyber exclusion.

What additional developments are likely in 2020?

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

- No consistent approach by markets 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/sub-limits.
- 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 usage of technology accelerates.

What is Marsh's recommended approach for addressing silent cyber modifications to P&C programs?

Marsh Position: Limit Gaps and Overlaps, Maximise Coverage and Potential Recovery

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 OK to exclude and include 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.

STAND-ALONE CYBER INSURANCE

- Typically superior (limits and breadth) to adding affirmative cyber sub-limits to non-cyber policies.
- Should cover losses arising from the confidentiality, integrity or availability of data or technology.
- $500M–$750M 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 continues to create solutions that seek to maximise coverage, restrict any coverage gaps or overlaps, and maximise potential recoveries.

- **Long Term** — We seek the adoption of clear, affirmative language that provides clients with full policy coverage across their traditional policies. For example, property damage that is covered under property policies, irrespective of the presence of technology in the causation of the loss.
- **Short Term** — We seek to protect clients' interests by adapting and amending the best wordings/clauses available and to challenge underwriters where that is resisted. In addressing the Lloyd's requirements, insurer wordings are currently allowing potential gaps to be created in clients' existing insurance programs at a time when new, emerging risks and technologies are driving clients' actual risks and cover requirements in the opposite direction.

What about stand-alone cyber coverage? Can it address any gaps in cover?

While there is some property damage capability and capacity available from cyber insurers, the best approach is to review your overall coverage requirements with your Marsh client team, as there are innovative stand-alone cyber covers which may provide additional protection and benefit to your organisation.

Stand-Alone Cyber Insurance Policies: Broad Coverage for Financial Risks, Limited Physical Damage Coverage

What elements of cyber risk are often covered by cyber policies?

CYBER COVER:

- 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 has limited capacity and this is the gap the traditional markets must fill).**

Where have insurance buyers historically found cover for physical loss or damage? Going forward, what approach is In their best interest?

CONSIDER:

- 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 230-person global team of specialised cyber risk management professionals work with clients in every market worldwide. We encourage you to please reach out to them early to help ensure you stay up to date on the full scope of solutions available.

For more information or 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 Cyber team:

KELLY BUTLER
Cyber Practice Leader, Pacific
Marsh JLT Specialty
kelly.butler@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.