MARSH JLT SPECIALTY

Recent Clarifications in Traditional Insurance Lines

Coverage Impact to Existing P&C Programmes due to "Silent Cyber" and Strategies to Maximise Coverage

June 2020

MARSH

Executive Summary
Traditional P&C Insurers Restricting Cover in Response to "Silent Cyber"

- Regulators in the UK identified "non-affirmative cyber" loss under traditional property and casualty (P&C) insurance as a threat to insurer solvency.
- Lloyd's of London mandated that, traditional P&C policies either expressly cover or exclude, these "silent cyber" exposures.
- Many major insurers around the globe have also reviewed their P&C policy wordings, whether subject to the Lloyd's mandate or not.
- Insurers are generally defaulting towards broad exclusionary language that can create significant coverage gaps in traditional P&C policies, **even for clients that purchase stand-alone cyber insurance**.
- Marsh has worked with many insurers to create alternative versions of exclusions and strategies to limit potential coverage gaps and maximise recovery.
- Clients should be aware of the potential gaps and how they impact all P&C insurance.
- Clients should consider purchasing stand alone cyber insurance but should understand that gaps may still exist.

Regulators Identified "Non-Affirmative Cyber" Coverage as a Threat to Insurer Solvency

Regulators and Insurers Are now Addressing This "Silent Cyber" Exposure

- Regulators and global insurers have reviewed non-affirmative cyber risks and exposures for many years.
- Rating agencies such as Fitch* have cited failure to manage these exposures as rating criteria.
- In the UK, the PRA and Lloyd's have driven the agenda and timeline as shown on the right.
- **In 2019, Lloyd's mandated that *all policies* must be clear on whether coverage is provided for losses caused by a cyber event. *Clarity is to be provided by either excluding, or affirmatively covering the exposure*, from all P&C policies.**
- EIOPA (European Insurance and Occupational Pensions Authority) likely to issue similar directive.

January 2019

- **UK Prudential Regulatory Authority (PRA)** letter to UK insurers.
- Required "action plans to reduce the unintended exposure that can be caused by non-affirmative cyber cover."

July 2019

- **Lloyd's Market Bulletin Y5258** set out new mandate.
- All policies to be **clear** on whether coverage is provided **for *losses* caused by a *cyber event***.
- This **clarity** should be **provided** by either **excluding coverage** or by **providing affirmative coverage**.
- Phase 1 effective date 1 January 2020.

January 2020

- **Lloyd's Market Bulletin Y5277** updated the timeline for the phased implementation across all lines of business.
- Phase 2 effective date 1 July 2020.
- Phase 3 effective date 1 January 2021.
- Phase 4 effective date 1 July 2021.

*Source: https://www.captive.com/news/2019/12/17/cyber-risk-analysis-inhibited-silent-cyber-risk-exposure

What Is "Silent Cyber" Coverage? Why Is This an Issue now?
New Technology and Increased Connectivity Creates new Risks

Technology continues to reshape the business landscape and intensify cyber risks for companies in every industry. Almost every asset is now remotely connected/controlled/managed, and therefore potentially vulnerable.

Cyber-attacks have moved beyond data breaches to sophisticated schemes designed to disrupt businesses and supply chains. The widespread nature of cyber-attacks also means that companies can suffer collateral damage even when they are not targeted.

Traditional insurers see claims stemming from cyber events that they had neither underwritten nor charged for, thus creating unmeasured exposure within insurer portfolios.

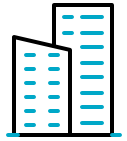
This new phenomenon is known as "silent cyber" and can arise in a number of ways.

For example, where…

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

What Are the “Silent Cyber” Risks for Traditional P&C Insurance?

Cyber Risks may Be Covered Under Various Lines of Insurance

Line of Business		Example Cyber Risks/Losses
Property Cover for material damage and business interruption, from physical loss or damage, to tangible property.		Malware attack scrambles data in 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 operators/owners incur liability.
General Liability Third-party bodily injury, property damage liability, advertising, and personal injury.		Cyber-attack causes heating system to overheat resulting in an explosion. Bodily injury and property damage ensue.
Directors and Officers Coverage for litigation or regulatory action arising out of a failure to disclose, misrepresentations, or breaches of fiduciary duty.		Publicly-traded company experiences data breach, ultimately leading to a stock drop, and a securities class action lawsuit follows.

Recent Market Response to "Silent Cyber" Has not Been Favourable to Coverage

Markets Have Often Defaulted to Overbroad Exclusionary Language

- The mandate and timeline from Lloyd's led to confusion as insurers rushed to comply.
- Lloyd's (and the PRA's) definition of cyber risk is problematic, and focuses on the type of event (malicious versus non-malicious), rather than on the resulting loss (physical or intangible).
- Insurers have tended towards applying exclusions rather than affirming cover, citing their concern over the potential for aggregation from a systemic loss.
- Cyber exclusion endorsements proposed on property policies have been inconsistent, and in some cases, overreach – potentially excluding any loss, simply because technology was somewhere in the chain of causation.
- Many proposed solutions ignore the fact that technology is integral to business operations across all sectors – and so cyber endorsements must be carefully drafted to avoid duplication or gaps in cover.
- Drafting appropriate, affirmative language for casualty, liability, and financial lines policies presents additional challenges with increased potential to restrict or compromise existing coverage.

Key is to ensure you understand the full potential impact of any proposed changes to your policy wording.

Buyer Options to Consider When Facing Proposed Cover Changes
When Traditional Lines Insurers Attach "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 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 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 greatest overall coverage.	• Gap filler policies tend to be expensive. • Coverage offered may not fully replace coverage taken away by the cyber exclusion.

Marsh Has Worked to Limit "Silent Cyber" Gaps and Maximise Potential Recovery

Marsh JLT Specialty Position - Maximising Coverage, Resolving Gaps/Overlaps

Traditional Policies

- Should cover resultant physical damage or bodily injury regardless of technology involvement
- Should cover malicious & 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

- **Superior*** (limits and breadth) to adding affirmative cyber sub-limits to non-cyber policies
- Cover losses arising from the confidentiality, integrity, or availability of data or technology
- $500 million-$750 million limit capacity
- Broad coverage for 1st and 3rd party risks:
  - Incident response.
  - Business interruption (non physical).
  - Data breach.
  - Data restoration, hardware replacement.
  - Cyber extortion.

* Source: see following slide 9.

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.
- Competitiveness of London market.
- Other policies purchased that already address the risk.

How Will "Silent Cyber" Impact Your Insurance Coverage Today?
Likely Challenges in 2020

P&C Lines: A lack of consistency amongst the markets across traditional lines regarding affirming/excluding/ sub-limiting cover, and a lack of agreement on language for exclusions.

Result: Differential language or approach across a single programme.

Cyber Market: A lack of consistency and relatively more limited market capacity among cyber product solutions compared to new P&C exclusions.

Result: New gaps may not be perfectly filled in the cyber market, either in respect of language or limits.

Minimising the Impact and Maximising Your Potential Recovery
Next Steps

- Review your cyber exposures: Contact your Marsh JLT Specialty client team and cyber team early to keep ahead of market developments.
- Keep updated via the dedicated **silent cyber page** on our UK website.
- Contact the Marsh JLT Specialty cyber team cyber.risk@marsh.com or any of the members of our dedicated UK silent cyber team (see next page).
- Your Marsh JLT Specialty cyber risk management contact is @XXXXXXXXXXX.

Marsh JLT Specialty UK - Silent Cyber Contacts

Placement

Dan Hearsum
dan.hearsum@marsh.com

Cyber

Sarah Stephens
Sarah.Stephens@marsh.com

FINPRO (Product)

Nicola Barnett
nicola.barnett@marsh.com

Energy/Power

John Cooper
john.cooper@marsh.com

Construction

Andrew Thornton
andrew.w.thornton@marsh.com

Stuart Freeman
stuart.freeman@marsh.com

Property

Ed Cotterell
Ed.Cotterell@marsh.com

James Moore
James.W.Moore@marsh.com

Felix Ukaegbu
Felix.Ukaegbu@marsh.com

Marine

Hull

James Reason
james.reason@marsh.com

Cargo

David Roe
david.p.roe@marsh.com

Andrew Watson
andrew.p.watson@marsh.com

Silent Cyber Project Manager

Keith Campbell
keith.campbell01@marsh.com

Appendix

“Silent Cyber”
Updated Lloyd’s Timetable as of January 2020

Phased compliance by class of business

Phase 1 – First-party property damage incepting on or after 1 January 2020

Class of Business

- Energy (construction, offshore/onshore property).
- Nuclear.
- Power generation.
- Cargo*.
- Fine art.
- Marine hull and war.
- Specie.
- Yacht.
- Difference in conditions.
- Property.
- Engineering.
- Livestock and bloodstock.
- Terrorism.

**Risk code V*

Phase 2 – Policies incepting on or after 1 July 2020

Class of Business

- Accident & health.
- Contingency.
- Space.
- Political risks, credit and financial guarantee.
- BBB/crime.
- Property (cat XL, pro rata, risk XS).
- Agriculture and hail.
- Livestock excess of loss.

Phase 3 – Policies incepting on or after 1 January 2021

Class of Business

- Airline.
- Aviation (products/airport liabilities, XL, cargo*, general).
- Directors & officers.
- Cyber (addressing clarity for any traditional coverage provided by extension to a cyber policy).
- Employers liability/WCA (non-US).
- Energy offshore and onshore liability.
- Extended warranty.
- Financial institutions.
- Legal expenses.
- Marine liability.
- Medical expenses.
- Medical malpractice**.
- UK motor and overseas motor.
- NM general liability.
- Pecuniary.
- Professional indemnity.
- Personal accident XL.
- Motor XL.
- Nuclear.
- Cargo.
- Terrorism.

- *Risk code VL*
- *** Risk code GH, GM, GN*

Phase 4 – Policies incepting on or after 1 July 2021

Class of Business

- Marine XL.
- Casualty treaty.
- Medical malpractice*.
- Employers liability/WCA (US).
- Marine war.

**Risk code GT*

PRA and Lloyd's Market Bulletin Y5258 Definitions

PRA Supervisory Statement 4/17 published 5 July 2017:

"This supervisory statement (SS) sets out the Prudential Regulation Authority's (PRA) expectations of firms regarding cyber insurance underwriting risk. For the purposes of this SS cyber insurance underwriting risk is **defined as** *the set of prudential risks emanating from underwriting insurance contracts that are exposed to cyber-related losses resulting from malicious acts (eg cyber attack, infection of an IT system with malicious code) and non-malicious acts (e.g. loss of data, accidental acts or omissions) involving both tangible and intangible assets."*

Lloyd's views policies where *no exclusion exists* **and** there is *no express grant of cyber coverage as* **non-affirmative** (i.e. containing "silent cyber").

Lloyd's defines **cyber risk** as 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.

Lloyd's definition of cyber risk:

"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."

1. The word "cyber" is not defined, yet it's incorporated within the body of the definition of cyber risk.
2. Loss of data and infection of an IT system with malicious code are two potential *results* of a cyber attack (malicious) or an accidental act (non-malicious), they are not, discrete malicious or non-malicious cyber *events*.
3. By trying to distinguish malicious from non-malicious, Lloyd's have inadvertently caused the underwriters to lose sight of the purpose of the mandate, which was to clarify whether ***coverage*** (i.e. the coverage that insurers have historically provided) extends when a cyber event is a direct or indirect cause of loss.