MARSH JLT SPECIALTY

DAC BEACHCROFT

Silent Cyber: Managing Cyber Coverage within a Changing Insurance Market

May 21, 2020

DAC BEACHCROFT

MARSH

Setting the Stage: Why Silent Cyber Should be on Your Agenda

Today's Agenda

Explain Silent Cyber

Review market and insurer changes – pros and cons

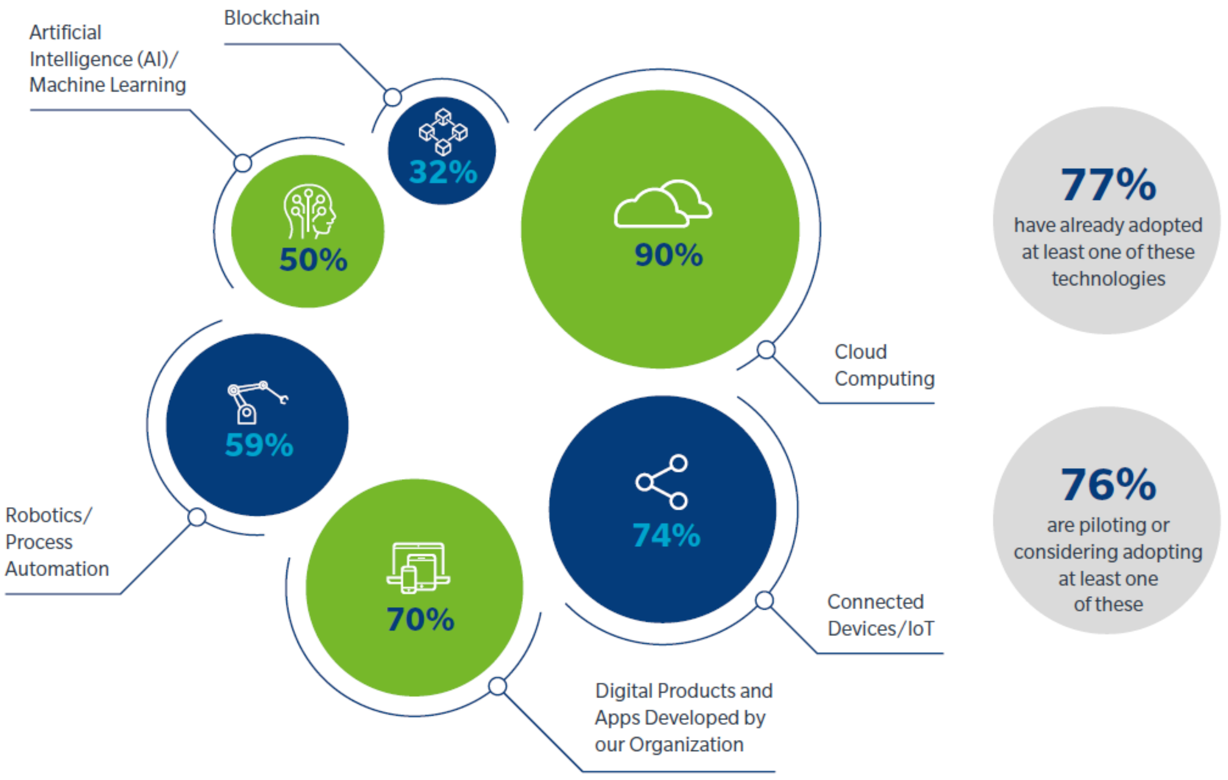
Analyze impact of changes on insureds' policies

Offer recommendations for organizations to secure cyber coverage

Silent Cyber: Situation Overview

- New technology brings new risks – and blurs the line between physical and cyber risk.
- Insurance (policy wordings) have traditionally lagged behind the evolution of technology.
- Insurers are now affirming or excluding cyber risks from non-cyber policies.
- Proposed exclusions are impacting coverage, sometimes overreaching to exclude physical risks merely because technology was in the chain of causation.

3 out of 4 companies are eagerly embracing new technologies, despite potential risks.



Source: Marsh Microsoft 2019 Global Cyber Risk Perception Survey

What is Cyber Risk?

What Is Cyber Risk?

"The possibility of loss or injury of, relating to, or involving data or technology"

What is Data?

Factual information (such as measurements or statistics) used as basis for reasoning, discussion, or calculation

Information in digital form that can be transmitted or processed

Information output by a sensing device or organ that includes both useful and irrelevant or redundant information and must be processed to be meaningful

What is Technology?

Computer Systems and networks, including cloud and data storage

Electronic devices, such as sensors, that are embedded in everyday objects or machinery and enable them to send and receive data, and/or to connect to internet (aka Internet of Things or IoT devices)

Automated machinery and equipment that can be controlled or programmed by computers

Computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and language translation (aka Artificial Intelligence or AI)

How Does Cyber Risk Manifest in Loss?

Consequences of Cyber Risk

Cyber Event

Malicious attacks or accidental events impacting data, computer networks, or technology.

Leading to:

Impact

- Encrypted Data
- Security Breach
- Privacy Violations
- Regulatory Investigations
- Phishing / Fraud
- Bricked Computers
- Property Damage
- Property Damage
- Property Damage
- Bodily Injury

Leading to claims for:

Consequence

- 1st Party Costs
- Loss of Income
- 3rd Party Liability
- Fines & Penalties
- Extortion Demands
- Negligence in Services
- Shareholder Litigation

What is Silent Cyber?

Consequences of Cyber Risk

Cyber Event

Malicious attacks or accidental events impacting data, computer networks, or technology.

Leading to:

Impact

Encrypted Data

Security Breach

Privacy Violations

Regulatory Investigations

Phishing / Fraud

Bricked Computers

Property Damage

Property Damage

Property Damage

Bodily Injury

Leading to claims for:

Consequence

1st Party Costs

Loss of Income

3rd Party Liability

Fines & Penalties

Extortion Demands

Negligence in Services

Shareholder Litigation

Defining Silent Cyber

Potential cyber exposures within traditional property and liability insurance policies which may not implicitly include or exclude cyber risk, but could theoretically pay claims for cyber losses in certain circumstances.

Instances when an insurance policy is triggered:

1. Cyber events as triggers for loss are not explicitly included or excluded;
2. Cyber exclusionary language within the policy is ambiguous;
3. Express cyber coverage grants are ambiguous or conflict with other policy wording.

Examples of Silent Cyber Triggers in Non-Cyber Policies

Property
Covers real and personal property 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.

A publicly traded company experiences a data breach, ultimately leading to a stock drop and a securities class action lawsuit follows.

Why are Insurers Concerned?

Insurers’ Concerns Driving Silent Cyber Changes

Non-affirmative wording in policies can result in inadvertent coverage of cyber exposures and thus unmeasured and unexpected risk in insurers’ portfolios:

- **Coverage disputes**
  - Claims stemming from cyber events under non-cyber policies that didn’t expressly address cover for cyber exposures.
- **Pricing**
  - Underwriting may not accurately consider cyber risks for insureds.
  - Risk exposure of insured not adequately measured.
  - Pricing doesn’t reflect cyber risk.
- **Accumulation**
  - “Silent” risk accumulation/aggregation not identified or measured.
  - Exposure to systemic risk.

ISN’T SILENT CYBER A GOOD THING FOR POLICYHOLDERS?

- Lack of clarity may create mistaken belief that coverage exists where it does not.
- Different interpretation by insurers of non-affirmative language can lead to claims disputed and legal action.

How Are Insurers & Regulators Responding?

Insurer & Regulator Actions to Address Silent Cyber Risk

- Risk concern over silent cyber exposure moved **UK regulators** to take steps to remove the "silence."
- **January 2019: Prudential Regulatory Authority (PRA)** instructed insurers to "have action plans to reduce the unintended exposure that can be caused by non-affirmative cyber cover."
- **July 2019:** **Lloyd's** Market Bulletin Y5258 required all policies be **clear** on coverage for **losses caused by a cyber event** – either **providing affirmative coverage** or **excluding coverage**.
  - Lloyd's **problematic definition of cyber risk** makes an arbitrary distinction between acts of misfeasance and malfeasance.
- **EIOPA** (European Insurance and Occupational Pensions Authority) likely to issue **similar directive**.
- **January 2020**: Lloyd's Market Bulletin Y5277 confirmed **phased implementation** across all classes. (*see next page*)
- Rating agencies such as **Fitch** have cited failure to manage non-affirmative cyber risks & exposures as **ratings criteria**.

LLOYD'S DEFINITIONS

- ***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.**
- ***Non-Affirmative Cyber:*** *policies where no exclusion exists and no express grant of coverage.*

**Defined by UK Prudential Regulation Authority*

Insurers are Complying with Silent Cyber Mandate by…

1 Affirming all physical cyber exposure within policy, regardless of technology involvement

Advantages:
- No coverage reduction or need for alternative
- Single policy for all triggers
- No disputes over cyber definition

Disadvantages:
- Sub-limits for intangible cyber losses
- Doesn't cover full gamut of cyber risk & sub-limits for intangible cyber losses may dissuade insureds from purchasing cyber policy required for full cover.
- Higher premium?

2 Affirming all physical cyber exposure but sub-limited

Advantages:
- Some coverage ensured

Disadvantages:
- Coverage previously unlimited now sub-limited

3 Excluding all cyber exposure

Advantages:
- Clarity

Disadvantages:
- Premium reduction unlikely
- Possible inadvertent exclusion of technology perils
- Physical loss cover may not be replicable

4 Excluding all cyber exposure but inserting write-backs for certain perils/losses

Advantages:
- Better than absolute exclusion

Disadvantages:
- Not as comprehensive as total cover affirmation
- May not write back in all previously covered perils
- Likely to attract additional premium

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

Phased Compliance By Class of Business

Phase 1: 1st Party Property Damage Incepting On or After 1 January 2020	Phase 2: Policies Incepting On or After 1 July 2020	Phase 3: Policies Incepting On or After 1 January 2021	Phase 4: Policies Incepting On or After 1 July 2021
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*	**Class of Business** • Accident & Health • Contingency • Space • Political Risks, Credit & Financial Guarantee • BBB/Crime • Property (Cat XL, Pro Rata, Risk XS) • Agriculture & Hail • Livestock Excess of Loss	**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 & 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*	**Class of Business** • Marine XL • Casualty Treaty • Medical Malpractice* • Employers Liability/WCA (US) • Marine War

Did Insurers Get It Right?

Problematic Initial Response by Insurers

- Confusion and haste as insurers rush to comply.
  - o Lack of consistency across markets / lines regarding affirming / excluding / sub-limiting cover.
- Flawed definition of cyber risk by PRA & Lloyd's.
  - o Focuses on type of event (malicious vs. non-malicious; tangible vs. intangible), rather than resulting loss.
- Overreaching exclusion of previously covered physical perils where technology is a cause.
  - Endorsements are inconsistent and overreach in excluding loss from previously covered physical perils simply because technology was in chain of causation.
- Markets tending toward overly broad exclusions vs. affirming cover.

BEWARE:

- Absolute cyber exclusions. No coverage for **any loss** if connected to a **cyber event**. (ex: CL380, LMA 5401, LMA5402, IUA -01-081, IUA -09-082)
- Exclusions that differentiate cover based on the type of **event** (malicious versus non-malicious), rather than the **resulting loss.** (non-physical or physical). (ex: LMA5400, LMA5403, AIMU2015)
- Exclusions that provide a carve back for only limited named perils such as fire or explosion, or that seek to impose a sublimit on cyber risk. (ex: NMA2914, LMA5400, CL437)
- Wordings that take away otherwise covered **ensuing loss** if **technology** or **data** is **implicated in** the chain of **causation**. (ex: LMA5400)

Policyholders’ Challenges for 2020

- No consistent approach amongst the markets across traditional lines regarding affirming / excluding / sub-limiting cover.
- Lack of consistency and market capacity among cyber product solutions in accordance with exclusions introduced.
- Addressing the gaps in cover that may be created by exclusionary language / sub-limits.
- Limitations in cover introduced by non-cyber insurers.

How Can These Issues Be Addressed?

Interim Solutions & Longer-Term Goals

Interim Solutions

- Where exclusions create gaps in coverage, insureds should consider purchasing cyber cover and look at insurer-created coverage solutions where a cyber policy cannot cover what is excluded.
- However these “bridge” solutions are not a long term solution as:
  - They can be narrowly worded.
  - Capacity outside traditional lines is limited, with typical maximum limits of £50 -100 million.

Ultimate Goal in Addressing Silent Cyber Risk

- Clarify and be consistent about what is meant by cyber risk, avoiding categorization into good (operational error) and bad (malicious intent) cyber.
- Ensure any exclusions applied are not triggered simply because a client uses technology to operate their business.
- Aim to cover events (including cyber events) leading to physical damage in a physical damage / property policy so there is unity of coverage and sufficient capacity.
  - Cyber and property underwriters should collaborate and develop appropriate modelling to carefully and clearly underwrite and rate for this, rather than simply excluding.
- Coverage overlaps should be avoided, either by careful drafting to delineate coverage or making other insurance clauses operate as clearly as possible.

What Should Policyholders Do?

Are There “Solutions” to Silent Cyber?

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.

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 greatest overall coverage.	• Gap filler policies tend to be expensive. • Coverage offered may not fully replace coverage taken away by the cyber exclusion.

Marsh & DAC Beachcroft Recommendations
Goals and Guidance for Policy Reviews

Traditional Policies

- Cover resultant physical damage or bodily injury regardless of technology involvement
- Cover malicious & non-malicious acts
- 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 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
- Covers losses arising from the confidentiality, integrity or availability of data or technology
- $500M - $750M limit capacity
- Broad coverage for 1st & 3rd party risks:
  - Incident response
  - Business interruption (non physical)
  - Data breach
  - Data restoration, hardware replacement
  - Cyber extortion
  - Physical damage: traditional markets need to fill this

Coverage Solutions in the Cyber Insurance Market

1

Inclusion of Property and/or Casualty risks in **bespoke blended policy** together with cyber risks.

2

Endorsement to **add Silent Cyber / physical cyber** risk to **cyber policy**:

- Differences in Conditions.
- Differences in Limits.

3

Endorsement to **include cyber risks in Property and/or Casualty** programs:

- Express coverage for otherwise excluded risks.
- One policy addressing full spectrum of risks.

4

Stand-alone Policy: **DIC or /Umbrella**:

- Express coverage for otherwise excluded silent cyber risks.

Pros:

- Express coverage for otherwise excluded risks.
- One policy addressing full spectrum of risks.

Cons:

- Market for Silent Cyber / physical cyber risk unable to provide limits equivalent to P&C insurers for traditional risk: **Tens of Millions vs. Billions.**

In Summary
Traditional P&C insurers Are Responding to Silent Cyber by Restricting Cover

- UK regulators identified “non-affirmative cyber” loss under traditional P&C insurance as a threat to insurer solvency.
- Lloyd’s mandated that traditional P&C policies either expressly cover or exclude “silent cyber” exposures.
- Insurers around the globe have begun to review their P&C policy wordings, whether subject to the Lloyd’s mandate or not.
- Insurers generally defaulting towards broad exclusionary language that can create significant coverage gaps in traditional P&C policies, **even for buyers that purchase stand-alone cyber insurance.**
- Organizations should be aware of potential gaps and how they impact all P&C insurance policies.
- Marsh has worked with insurers to create solutions and alternate versions of endorsements and strategies to limit potential coverage gaps and maximize recovery.

Contacts and Resources

Marsh UK Silent Cyber Contacts

MARSH

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

Marsh US Silent Cyber Contacts

Cyber

Elisabeth Case
Elisabeth.Case@marsh.com

Bob Parisi
Robert.Parisi@marsh.com

Tim Marlin
Timothy.Marlin@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

FINPRO

Robert Salinardo (Bermuda)
Robert.L.Salinardo@marsh.com

Sarah Downey
Sarah.D.Downey@marsh.com

Barry Mansour
Barry.Mansour@marsh.com

Property

John Hughes
John.F.Hughes@marsh.com

Scott Patterson
Scott.M.Patterson@marsh.com

Casualty

Burt Garson
Burt.M.Garson@marsh.com

Jesse Paulson
Jesse.Paulson@marsh.com

DAC BEACHCROFT Silent Cyber Contacts

Julian Miller
Jmiller@dacbeachcroft.com

Thank You!

MARSH JLT SPECIALTY

DAC BEACHCROFT

Silent Cyber: Managing Cyber Coverage within a Changing Insurance Market

May 21, 2020

DAC BEACHCROFT

MARSH