GUY CARPENTER

Grappling With The “Silent Cyber” Peril

What Is It? Why Is It A Problem? What Can We Do?

Jamie Pocock

Head of GC Cyber Analytics – International

GRAPPLING WITH THE “SILENT CYBER” PERIL

1 WHAT IS SILENT CYBER?

2 WHERE DID SILENT CYBER COME FROM?

3 HOW IS THE MARKET REACTING TO SILENT CYBER?

4 HOW CAN WE QUANTIFY SILENT CYBER?

5 CONCLUDING THOUGHTS

What is “Silent Cyber”?
An Introduction to the Concept

Traditional lines insurers have begun to see claims stemming from cyber risks, risks that they had neither underwritten to nor charged for, creating unmeasured exposure in their portfolios. This new phenomenon of non-affirmative coverage for cyber risk in non-cyber policies is known “**silent cyber**”.

Instances when an insurance policy is triggered where:

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.

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 and Officers

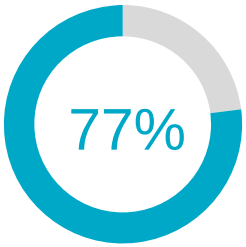
Coverage for litigation or regulatory action arising out of a failure to disclose, misrepresentations, or breaches of fiduciary duty.

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

Silent cyber is a broad term to encompass unintended exposure to the cyber peril

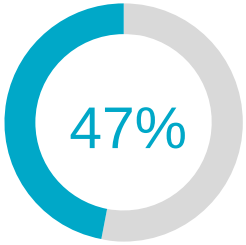
Where Did Silent Cyber Come From?
The Ambiguities of Coverage

‘Silent’ Cyber Risk is a Key Market Growth Inhibitor

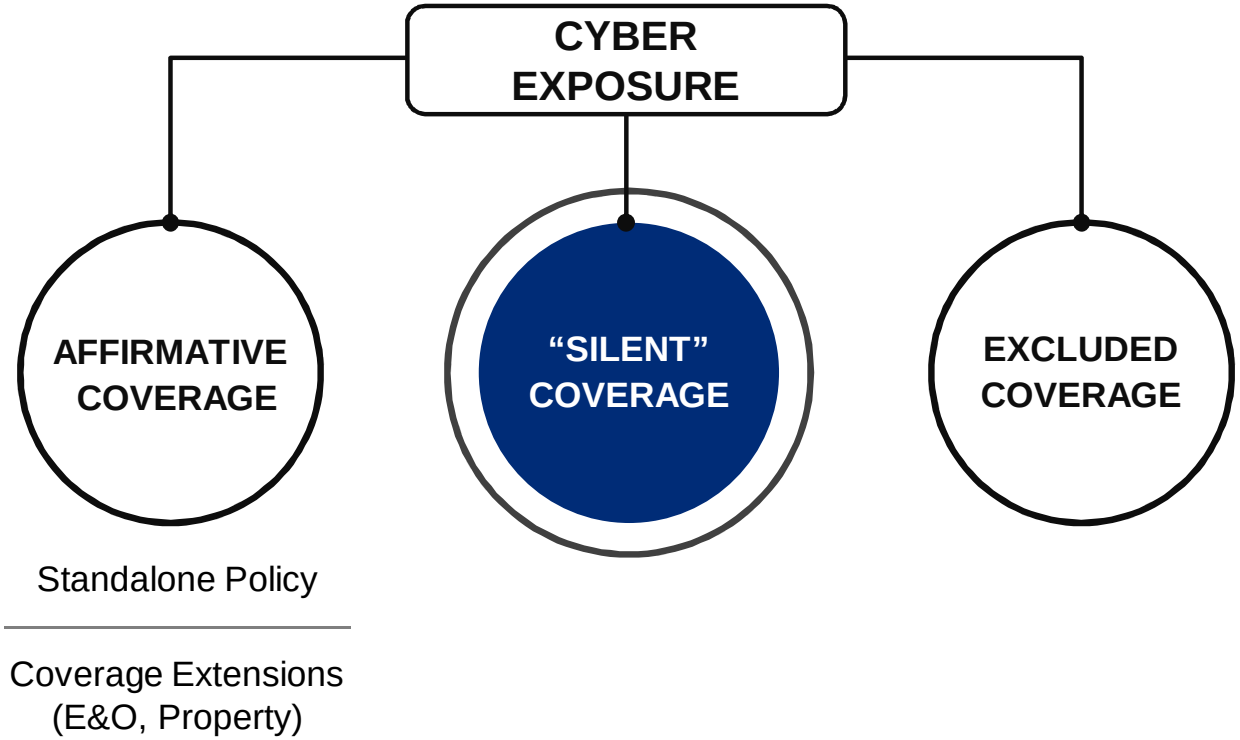


…of cyber risk insurance brokers and insurers believed that the insurance industry needs to urgently address non-affirmative cyber or ‘silent cyber’ in a deeper, more meaningful way

Cyber Perils Disconnected From Policy Clause



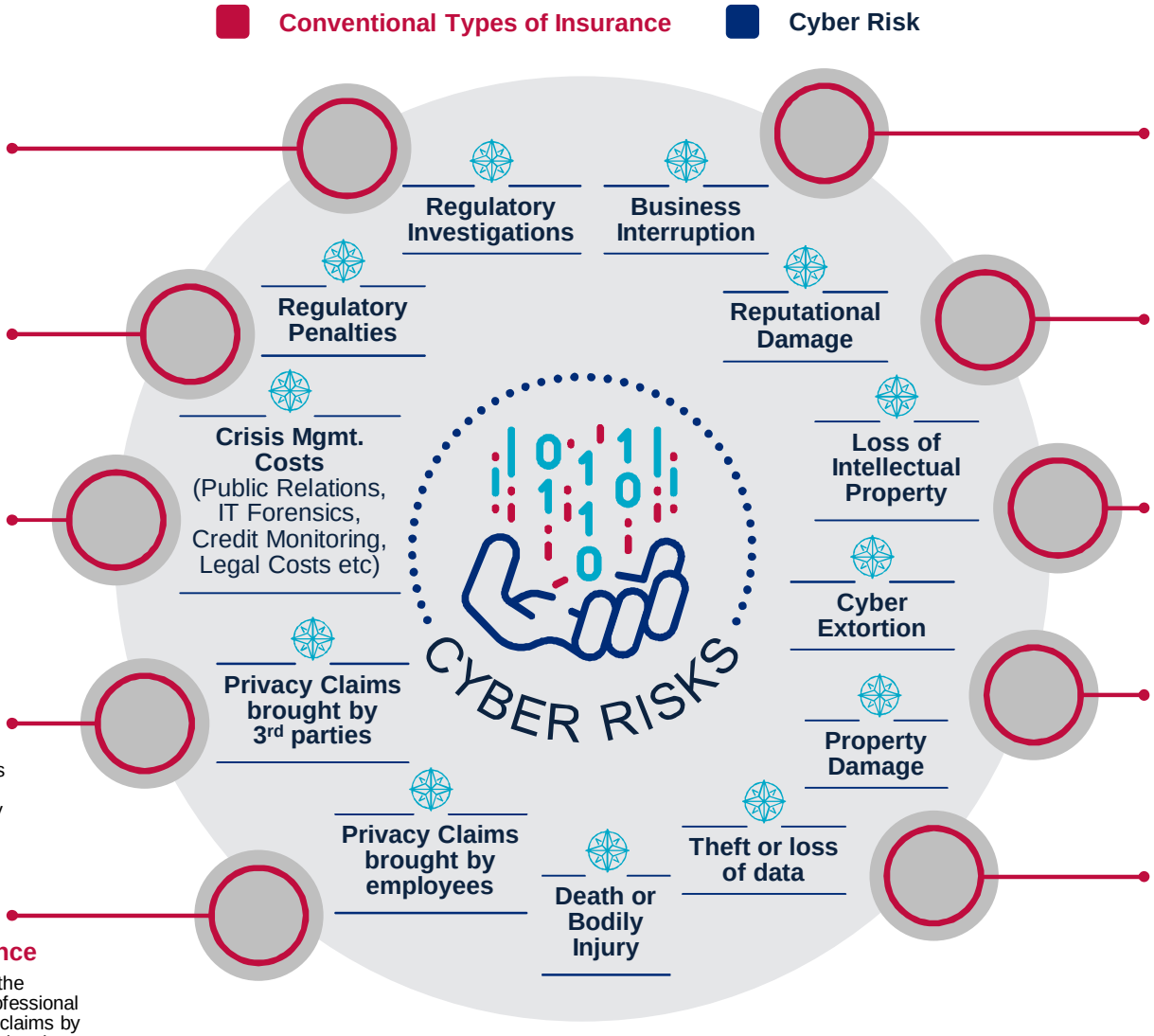
…of respondents admitted to having no clear connection between core cyber peril events and cyber risk insurance cover elements in their policy wording



CYBER EXCLUSIONS

that can be difficult to fashion to exclude all possible exposures from all possible cyber events

Where Did Silent Cyber Come From?
Lines of Business Exposed to Cyber Risk



Property Damage & Business Interruption Insurance

[Trigger for cover is usually physical loss of or damage to property]

General Liability Insurance

[Only covers bodily injury and physical property damage (i.e. not loss of data or business interruption losses which result from non-physical loss or damage]

Product Recall / Product Insurance

[Only covers bodily injury and physical property (i.e. not loss of data or business interruption losses which result from nonphysical loss or damage]

Directors' and Officers' Liability Insurance

[Primary focus of cover is on investigations and claims made against directors and officers, not against the organisations they are employed by]

Professional Indemnity Insurance

[Trigger for cover is usually negligence in the performance of professional services] [Professional indemnity insurance will not usually cover claims by employees] [Cover is often restricted to claims by clients or customers, often not third parties]

Aviation Insurance

[Specific exclusions likely to apply, in the context of malicious or terrorist acts, subject to buy-back]

Marine Insurance

[Specific exclusions likely to apply, in relation to "computer" use or operation as a "means for inflicting harm"]

IT / Computer Insurance

[May only cover loss to physical computer hardware]

Crime Insurance

[Trigger for cover is often some form of wrongdoing] [Monetary loss often required before cover]

Employment Practices Liability Insurance

[Cover only provided for certain types of claim brought by employees]

Source:
Cyber Risks and Insurance - An Introduction to Cross Class Cyber Liabilities [January 2016]

How is the Market Reacting to Silent Cyber?
The Silent Cyber Timeline

Thematic Review carried out by the PRA

Expression of concerns about the materiality of silent cyber as a risk to re/insurance companies recommending that firms needed to

- identify clear ways of managing "silent" cyber risk
- set clear appetites and strategies that would be owned by boards
- invest in cyber expertise

2016

2017

NotPetya and WannaCry

PRA - Supervisory Statement SS4/17

- Setting out expectations of firms regarding cyber insurance underwriting risk

PRA - 'Dear CEO' Letters

- (Re)Insurers should have action plans to reduce the unintended exposure that can be caused by non-affirmative cyber cover

Early 2019

Mid 2019

Lloyd's Bulletin Y5258

- Requiring clarity of coverage for cyber exposures in all policies
- To be adopted for all first-party property damage business incepting on or after 1 January 2020

Lloyd's Bulletin Y5277

- Update to Y5258 reiterating Lloyd's focus on driving the eradication of silent cyber from traditional line
- Update to the phasing approach

2020

Ongoing

- Market engagement and feedback
- Insurer/Reinsurer engagement
- Wording reviews
- LMA Proposed Clauses

Reaction to silent cyber has been an iterative process with key market stakeholders

How is the Market Reacting to Silent Cyber?
Lloyd's Market Update

The Lloyd's Market Bulletins have set out a new requirement for all policies to provide clarity regarding cyber coverage by either excluding or providing affirmative coverage.

For the purposes of implementing the requirements, cyber risk is defined by Lloyd's 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 (e.g. loss of data, accidental acts or omissions) involving either tangible or intangible assets.

- **Lloyd's have set a timeline for completion of this 'affirmative coverage' requirement in four phases. It is being implemented using a phased approach by class of business during 2020 and 2021.**
  - **Phase 1 – First Party Property**
    - Including but not limited to energy, cargo, marine hull, property D&F, and engineering
    - **Policies incepting 1 January 2020**
  - **Phase 2 – Property and Speciality**
    - Including but not limited to accident & health, contingency, space, political risks, and property treaty
    - **Policies incepting 1 July 2020**
  - **Phase 3 – General**
    - Including but not limited to aviation, D&O, motor, and various liability classes
    - **Policies incepting 1 January 2021**
  - **Phase 4 – Casualty and Marine**
    - Including but not limited to marine XL, casualty treaty, medical malpractice, and EL
    - **Policies incepting 1 July 2021**

The Lloyd's Market is opting for a multi-stage approach to bringing greater clarity to the peril

How is the Market Reacting to Silent Cyber?
Market Coverage Response

Although the LMA, the IUA and various bodies have issued model clauses there has been no universal adoption of one clause or approach by the whole market.

Addressing Silent Cyber Exposure	
Affirmation	Positively affirm where cyber exposure exists in the policy.
Affirmation but with sub-limits of the cover available	Positively affirm where cyber exposure exists in the policy and cover will then be provided with a sub-limit to that element of cover.
Exclude all exposure	Exclude on an absolute basis any loss from cyber exposure. Typically, these cyber exposures will be defined.
Exclude, but write back in specific areas of cover	Exclude on an absolute basis any loss from cyber exposure, but provide specific write-backs for a list of perils according to appetite.

How is the Market Reacting to Silent Cyber?
Action taken by Notable Market Participants

	Allianz	AIG	Lloyd's
Stance on Silent Cyber	"We will **make it clear how cyber risks are covered in traditional policies** and for which scenarios a dedicated cyber insurance solution is needed. The new strategy also **responds to growing concern from regulators and rating agencies** about cyber exposures in insurers' portfolios."	"American International Group Inc. will make **all of its cyber insurance coverage explicit.** The shift from silent cyber was designed not only to allow AIG to understand its own exposure better, but also to **make it clearer to clients what is and is not covered** under its cyber policies."	"For the avoidance of doubt, **Lloyd's view policies where no exclusion exists and there is no express grant of cyber coverage as 'non-affirmative'.** In all these cases action should be taken to provide clarity of coverage for customers to comply with this requirement," Lloyd's said.
Timing / Implementation Process	• The new wordings will be implemented from 1 January for all new AGCS business, and beginning 1 April for AGCS renewal business. • By 1 January 2020, the new underwriting approach will be in force for all Allianz P&C entities globally.	• "It had taken AIG around three years to ensure that it had identified the cyber-exposed areas in its products, a process completed in mid-2018." • AIG announced that starting from Jan. 1, 2019 new policies will begin to tackle the problem of silent cyber risk, however implementation has been inconsistent	• For first-party property damage policies incepting on or after January 1, 2020, underwriters are required to ensure all policies affirm or exclude cyber cover. This applies to new and renewal policies, as well as cover holder arrangements, line slips and consortia. • Liability and treaty reinsurance: the requirements will come into effect in two phases during 2020/21.

How can we Quantify “Silent Cyber”?
The Prudential Regulation Authority Stress Test

The PRA intends to engage with the general insurance industry to develop a cyber-scenario in time for the 2022 Insurance Stress Test exercise. To prepare for this, an exploratory cyber scenario was included in the 2019 IST to assess the industry’s ability to estimate sources of loss for such an event.

The implied losses from this scenario were, for many firms, comparable with the losses from their NatCat events. This illustrates the increasing materiality of cyber risk.

There was a divergence in materiality of non-affirmative cyber impact across firms that suggested a patchy ability to assess such losses.

Results are indicative of differences in firms’ perceptions of risk, illustrated by divergence in traditional products deemed exposed to the event:

- Five out of 20 firms attributed majority of loss to property covers
- Nine firms judged that the cost would mainly come from Errors & Omissions (E&O) and Directors & Officers (D&O) policies.

The exercise has reinforced concerns on the ability of some firms to assess and manage cyber exposures. There was material divergence in expertise, data, models and parametrisation in the estimation of both ‘affirmative’ and ‘non-affirmative’ cyber claims.

Chart 5: Ratio of Net losses to Eligible Own Funds (EOF) at 31/12/2018: interquartile range(a)

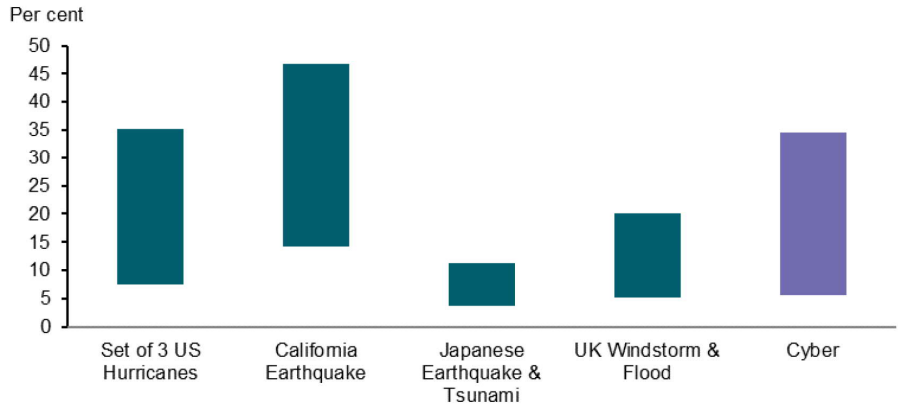
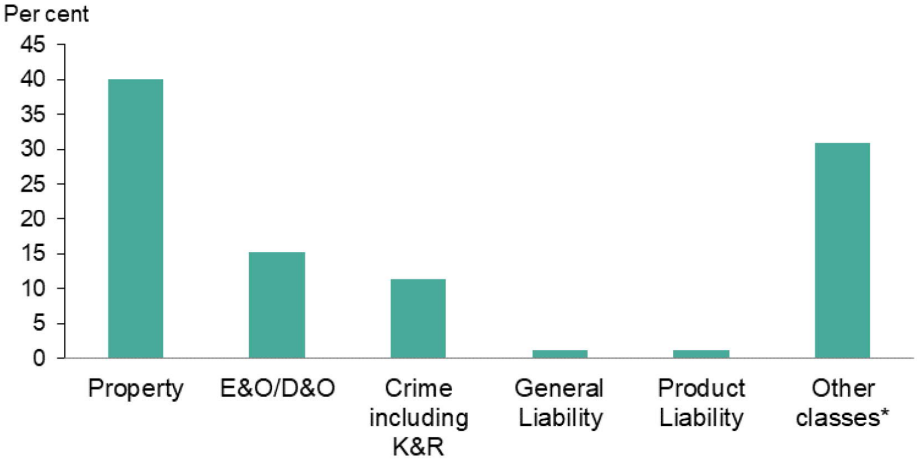


Chart 6: Non-affirmative cyber losses product breakdown(a)



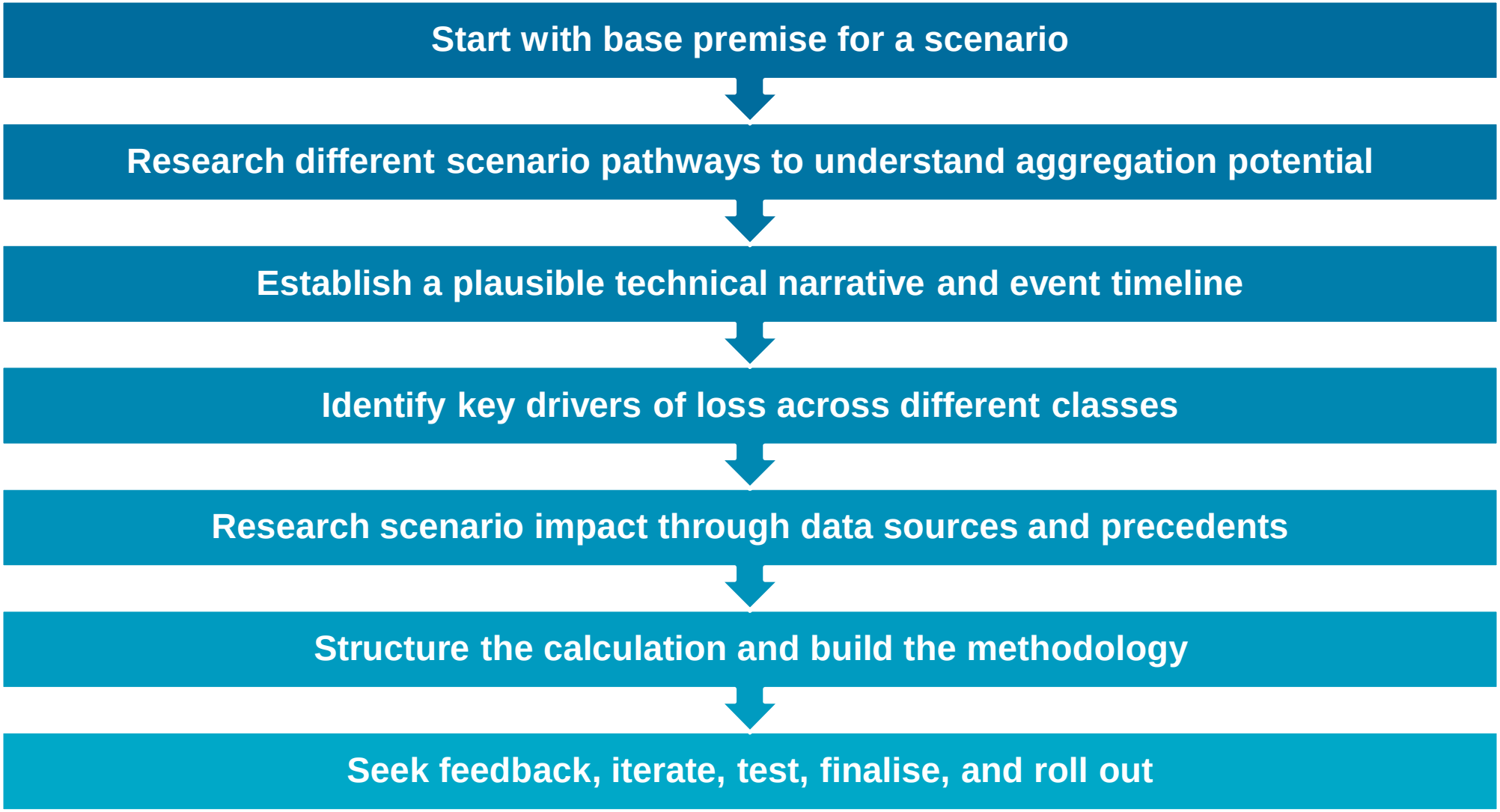
How can we Quantify “Silent Cyber”?
Using Traditional Techniques, and Moving Outside the Comfort Zone

The role of analysts is a very important one in assessing, quantifying, and modelling this type of peril exposure

- **Examine the peril in depth**
  - Understand that “cyber” can mean many different things, all of which may be relevant when considering the impact across different classes of business
  - **Understand better the nuances of cyber**: first and third party, malicious / non-malicious aspects, direct causes vs. supply chain and infrastructure-based triggers, OT vs. IT systems exposure, data security vs. disruption.
- **Focus on coverage**
  - To effectively model the risk requires a multi-dimensional approach; it is important to play a bigger role dealing with the nuts and bolts of insurance coverage
  - Analysts with technical skills can lead the charge in the deployment of **emerging tools and techniques** to gather coverage information to be in a position to quantify the peril
- **Collect incident and claims information from inside and outside the organisation**
  - Increasingly the market is seeing cyber-triggered losses across lines of business. Common classes can include D&O, property, K&R, general liability
  - Claims can be categorised for the presence or absence of a cyber trigger to create **a valuable source of silent cyber data**
- **Examine exposure using plausible aggregation scenarios**
  - Use discussions with peril and coverage experts to understand the vulnerabilities on a portfolio for the coverages offered. Focus on constructing a narrower selection of scenarios initially with significant depth, before branching out for more breadth
  - **Review frequently**; take stock of incidents or shifts in the risk landscape that validate, better inform, or challenge scenario selection

Think outside of the box! Do not be shackled by traditional actuarial methods!

How can we Quantify “Silent Cyber”?
Deep Dive - The Development Process for a Scenario



Concluding Thoughts

How to Manoeuvre from an “Unknown Unknown” to a “Known Unknown”

The problem isn’t going away – **don’t defer action** until later

Understand the difference between the cyber peril and the cyber product

See the “silent cyber” phenomenon as an **opportunity** to better understand risk as a concept

Collaborate: work with specialists that you are not use to working with to construct a balanced view

Get comfortable talking about the nuances of **insurance coverage** in detail

Play to your strengths: build a data-driven exposure and experience view of the risk

But **understand the limitations** of those approaches and communicate uncertainties clearly

Refine, test, iterate, cross-examine, and validate to build an **effective process**

Make it actionable: look for the outcomes as to how proactively shape the business

Actuaries have a very significant role to play in shaping the market’s approach to this peril

Important Disclosure

Guy Carpenter & Company, LLC provides this document for general information only. The information and data contained herein is based on sources we believe reliable, but we do not guarantee its accuracy, and it should be understood to be general insurance/reinsurance information only. Guy Carpenter & Company, LLC makes no representations or warranties, express or implied. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such. Please consult your insurance/reinsurance advisors with respect to individual coverage issues.

Readers are cautioned not to place undue reliance on any calculation or forward-looking statements. Guy Carpenter & Company, LLC undertakes no obligation to update or revise publicly any data, or current or forward-looking statements, whether as a result of new information, research, future events or otherwise. The rating agencies referenced herein reserve the right to modify company ratings at any time.

Statements concerning tax, accounting or legal matters should be understood to be general observations based solely on our experience as reinsurance brokers and risk consultants and may not be relied upon as tax, accounting, regulatory or legal advice, which we are not authorized to provide. All such matters should be reviewed with your own qualified advisors in these areas.