MARSH JLT SPECIALTY

Cyber Insurance in 2025

24 July 2019

Sarah Stephens
Cyber, Media & Technology Practice Leader

MARSH

The Baseline

Understanding the Baseline
2019 Cyber Misconceptions

As businesses become increasingly reliant on technology, their cyber risk exposures and the potential economic loss they could incur from a cyber attack has grown dramatically.

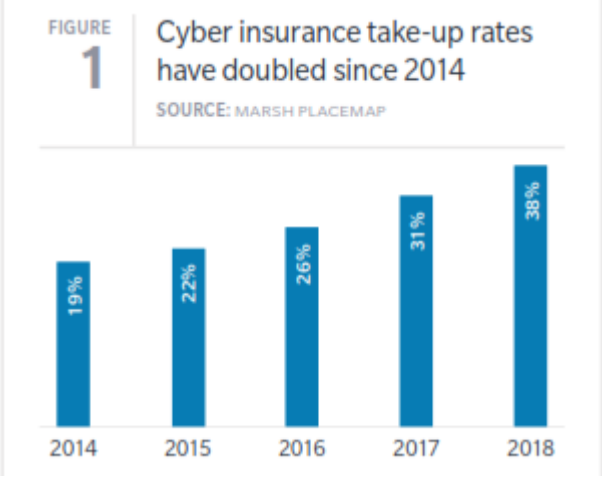
For this reason, cyber has now become one of the top 5 business risks and cyber insurance has become a necessity.

Recent media attention has left a question mark over the effectiveness of cyber insurance. However, these reports usually conflate traditional policies, like property, casualty and crime insurance, with standalone cyber.

Standalone cyber insurance has consistently paid claims since its inception 30 years ago. In contrast, traditional coverage was not designed to respond to cyber risks, so the chances of claims being denied are higher.

Understanding the Baseline
Increasing Appetite, Claims and Payouts

The number of Marsh clients buying dedicated cyber insurance has doubled over the past five years, with nearly 40% now purchasing cyber policies.



The development of coverage options is attracting a wider range of buyers; with highest growth among the hospitality, manufacturing, education, power and utility sectors.

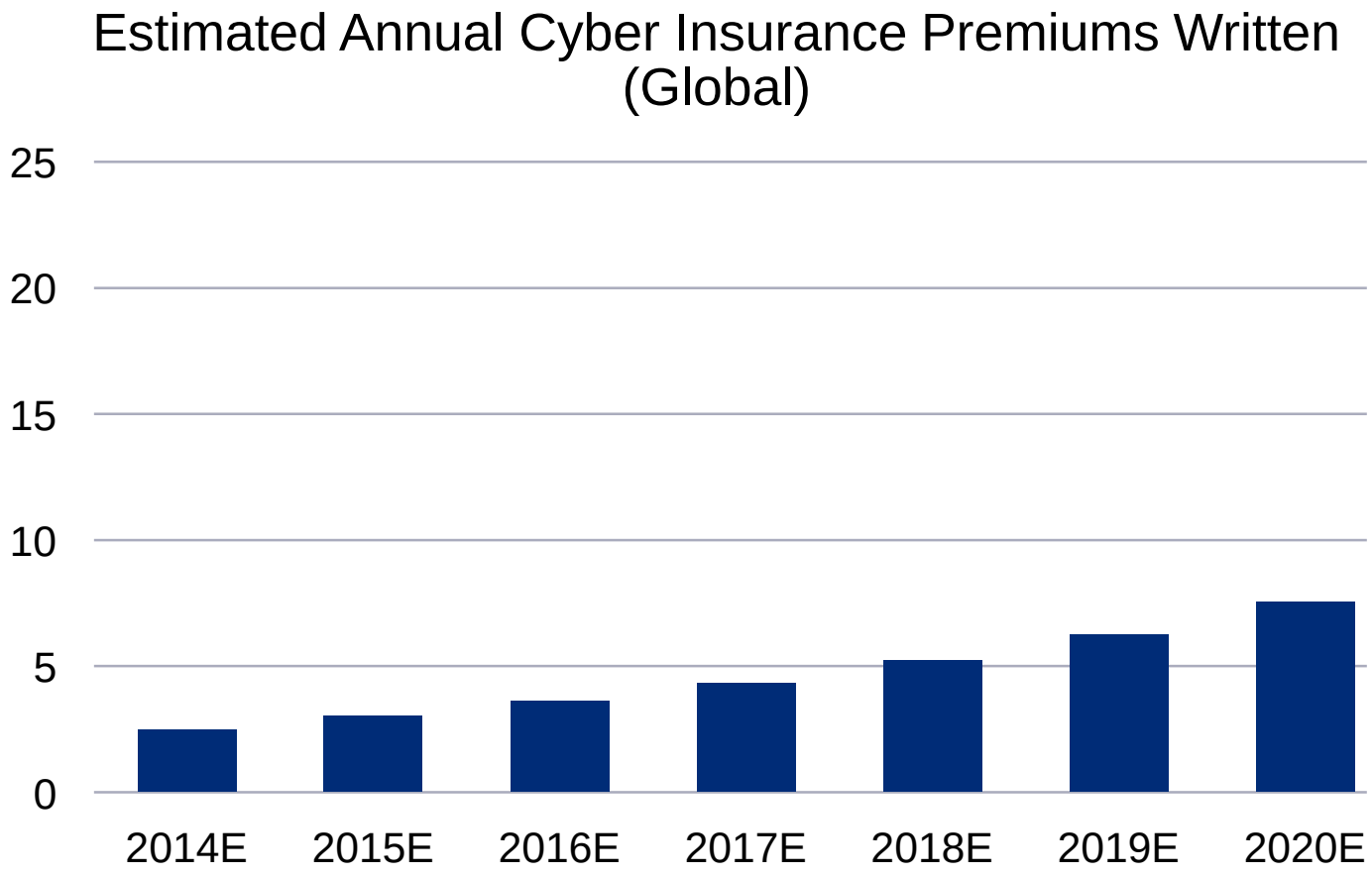
Understanding the Baseline
Claim Statistics

According to CreditSights, US insurers paid cyber claims totalling US$394 million in 2018, up from US$226 million the previous year.

- AIG paid 2,000+ cyber claims globally in 2018.
- Beazley covered 3,300+ data incidents in 2018 (and 10,000+ since 2009).
- In 2018, specialty cyber insurer CFC paid 1,000+ cyber claims and expects that number to increase by 50% in 2019.
- Hiscox dealt with 1,000+ cyber claims in 2017, a 1700% rise on 2013.

These figures point to an increasing recognition of cyber insurance as an effective and responsive way to cover cyber event losses.

Understanding the Baseline
Cyber Market Growth



Source: PwC, Lloyds, BI Intelligence Estimates, 2015

MYTH: “Cyber Insurance Does Not Cover Human Error”

REALITY: While cyber insurance was primarily designed to address malicious cyber incidents, it has evolved to cover a wide range of operational and human risks, including;

- Social engineering.
- Accidental disclosure.
- Loss of a laptop or device.
- Rogue employees.
- Failed updates and system migration.

Generally, cyber policies do not exclude coverage for accidental errors or omissions. Many cyber policies affirmatively cover such losses through system failure or administrative error coverage grants.

MYTH: "Data Breach Costs Focus on Legal Liability"

REALITY: Data breach insurance is the most established aspect of cyber insurance. Coverage is broad, particularly for first-party breach response costs, which can include;

- Legal.
- Crisis management.
- Call centre.
- Forensics.
- Credit monitoring.
- Notification expenses.

Cyber insurance will generally also cover the expenses associated with business interruption and data loss events.

MYTH: "Insurers Dictate Which Incident Response Providers & Advisors Are Used"

REALITY: While most cyber insurers have a recommended panel of service providers (legal counsel and vendors), many are willing to accommodate an insured's existing or preferred providers.

Some insurers will even allow policyholders to have absolute discretion in their choice of vendors.

MYTH: “Business Interruption Cover is Limited”

REALITY: Business interruption cover has evolved considerably to reflect the nature of how companies function today.

Cover will typically extend to the overall financial impact to the business, beyond just the duration of the cyber event.

Many policies will also cover losses resulting from a system failure or technology disruption at an insured’s IT vendors or within its supply chain.

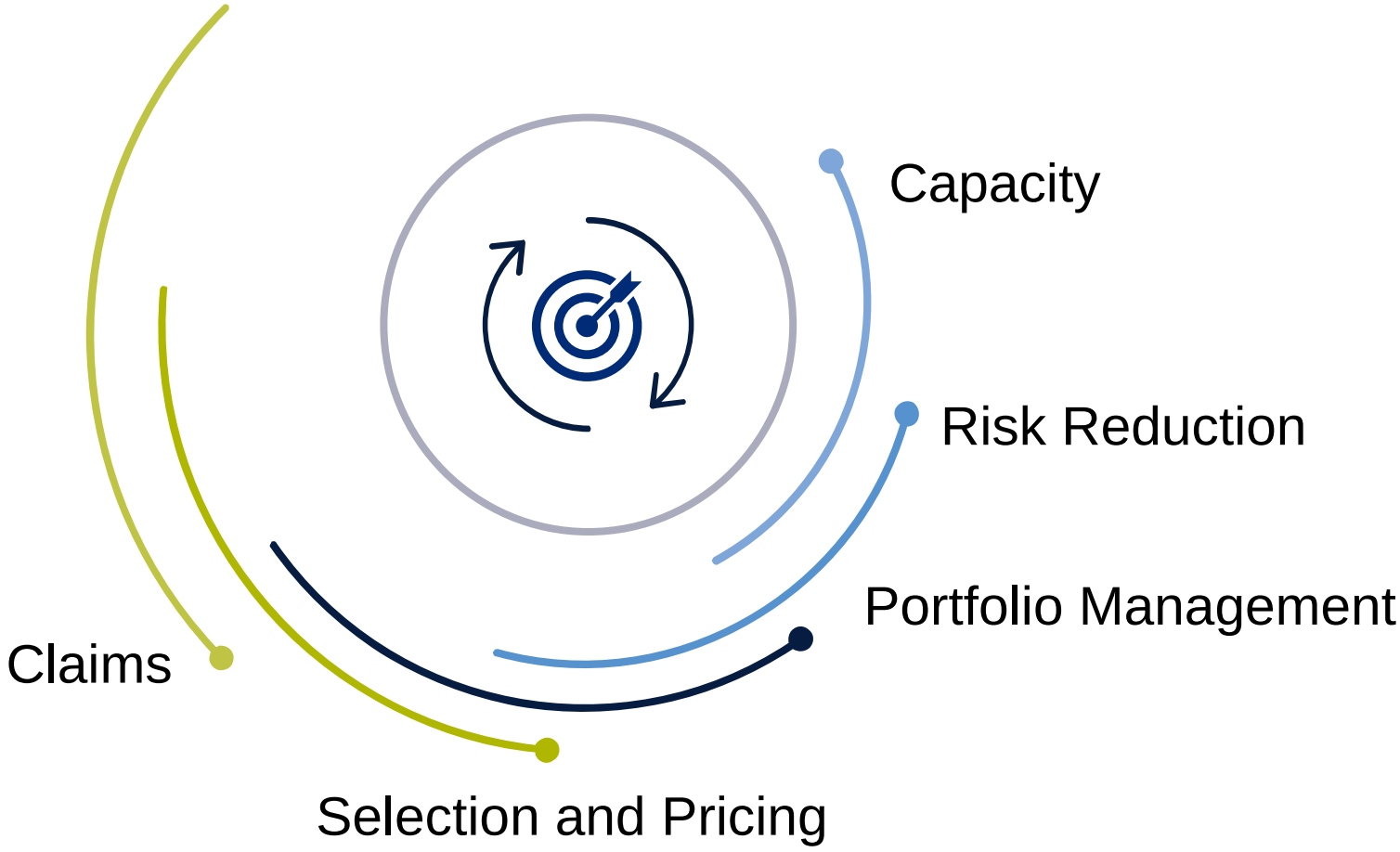
MYTH: “Cyber Insurance Excludes Recent Technology or System Upgrades”

REALITY: A robust cyber insurance policy can contemplate system upgrades where such best practice is the most cost-effective solution.

Cyber insurers embrace insureds that view security as a journey, not a destination.

Cyber Insurance Innovation

Cyber Insurance Innovation
Major Opportunities



Cyber Insurance Innovation
Claims

Claims Reporting

- The time sensitive nature of cyber incidents requires a faster claims response.
- Late notice or misunderstanding of incident response requirements causes claims disputes.
- Connecting SIEM systems to insurers in real time could automate incident reporting and minimise claim costs.
- Imagine if the incident response team called the insured instead of the other way around.

Cyber Insurance Innovation
Selection and Pricing

Pricing Models

- Insurers are reliant on their own loss data and brokers are reliant on industry surveys.
- Data is not well indexed, interoperable, or transparent.
- **The result is that pricing models are only using loss data to a fraction of its potential utility.**

Underwriting Information

- Underwriting data gathering process is not automated.
- Reliance on outside-in approaches is increasing.
- Advances in the automated inside-out method.
- Risk reduction correlation to premium savings.

Cyber Insurance Innovation
Portfolio Management

Aggregation Visualisation/ Modelling

- Quantify and visualise silent cyber.
- Aggregation to the Cloud and other vendors.
- Common vulnerabilities across the book.

Dynamic Risk Analysis

- In a dynamic risk area, the aggregate and specific exposure can change day-to-day.
- We accumulate risk data during the policy period.
- Pre-loss alerts are sent directly to policyholders (those who don't already have advanced threat intelligence/SIEM).
- Future state: dynamic pricing and risk management?

External Forces

External Forces
Silent Cyber – The Phenomenon

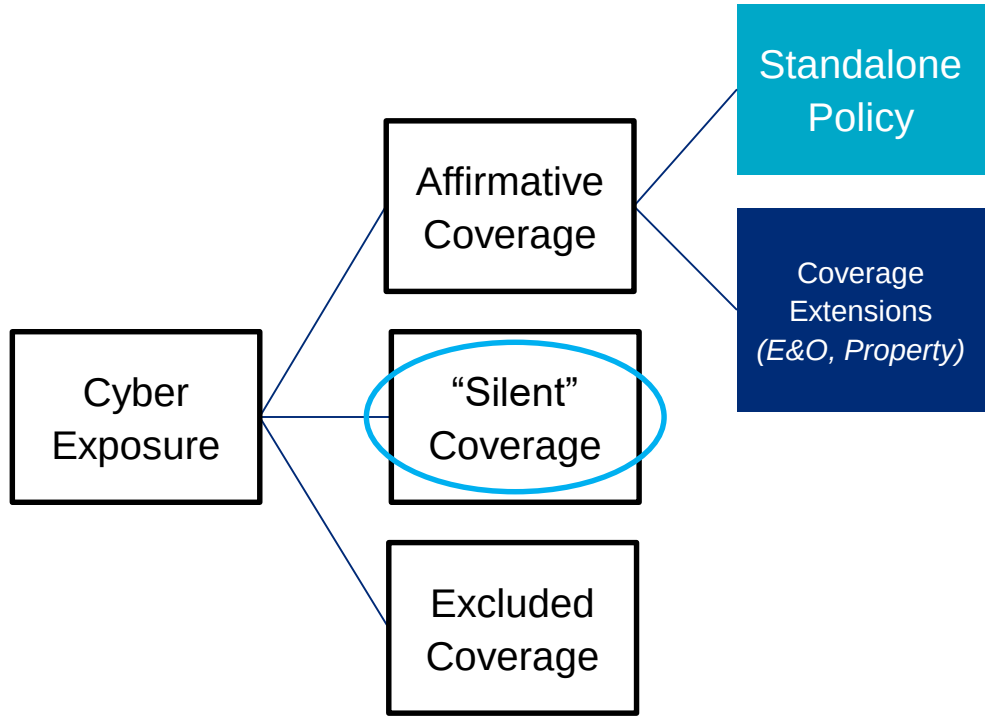
‘Silent’ Cyber Risk is a Key Market Growth Inhibitor

77% of cyber risk insurance brokers and insurers believe 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 Clauses

47% of brokers and insurers admitted to there being no clear connection between core cyber peril events and the elements of cyber risk insurance cover in their policy wordings.

It can be difficult to use cyber exclusions to exclude all possible exposures from all possible cyber events.



External Forces
What That Means

FOR BUSINESSES:

Contract certainty is still lacking and coverage interpretation remains in question.

FOR INSURERS:

There may be unknown, but potentially sizeable cyber exposure on their portfolios.

FOR REINSURERS:

There is little silent capacity to deploy, given the sizable lines they may already have on the standalone product and other possible lines of impacted business.

FOR ALL:

This ambiguity can lead to more antagonistic settlement processes in the event of a cyber related loss.

THE RESULT

The market may not grow as needed and is currently not equipped to address silent exposure through pure risk transfer.

Alternatives to traditional reinsurance, such as insurance-linked securities (ILS) and industry loss warranties, could step in to cover the breach, but it could be some time before the capital markets' investors backing these types of products get comfortable with the risks.

- **SNL May 2018**

External Forces
New or Upcoming Regulations

International
- EU General Data Protection Regulation (GDPR).
- Similar: Brazil, Japan, India and Thailand.

US Federal
- SEC Cybersecurity Disclosure Guidance.
- GSA Cybersecurity Contractor Reporting Rules.
- Health Insurance Portability and Accountability Act (HIPAA).
- SOX Cybersecurity Systems and Risks Reporting Act.
- DoD DFARS Contractor Standards.

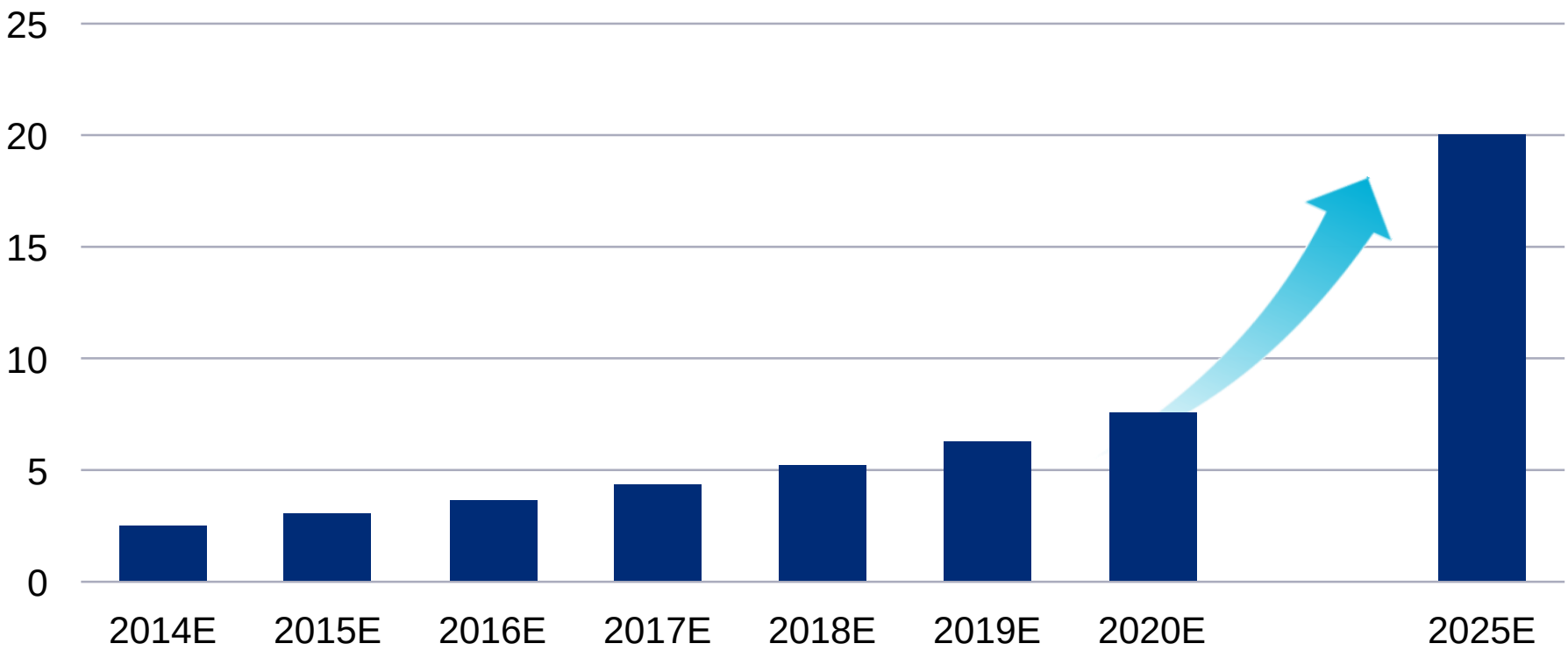
US State
- NYS DFS Cybersecurity Regulation for Financial Institutions.
- Illinois Biometric Information Privacy Act.
- California Consumer Privacy Act.
- California Internet of Things Cybersecurity Law.

External Forces
Changing Regulatory Scope Beyond a Privacy Breach

- Expansion beyond data protection/event response.
- Shift from reactive to prescriptive (GDPR).
- New frontiers: biometric privacy (BIPA).
- “Old” laws, retargeted to cyber issues (SOX).
- Non-cyber authorities issuing cyber guidance (SEC, NYS).

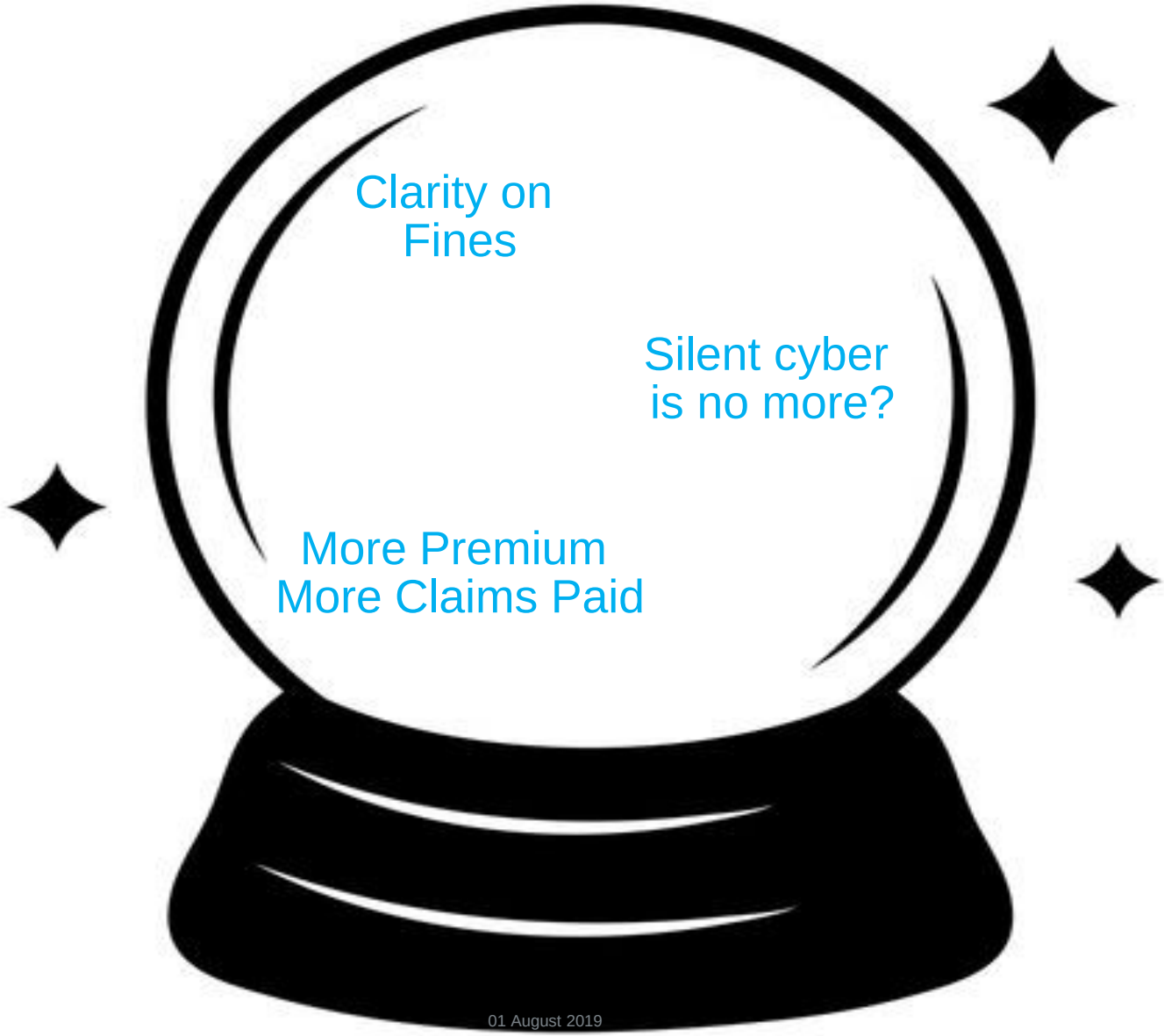
2025 Vision

2025 Vision
Estimated Annual Cyber Insurance Premiums Written (in $B)



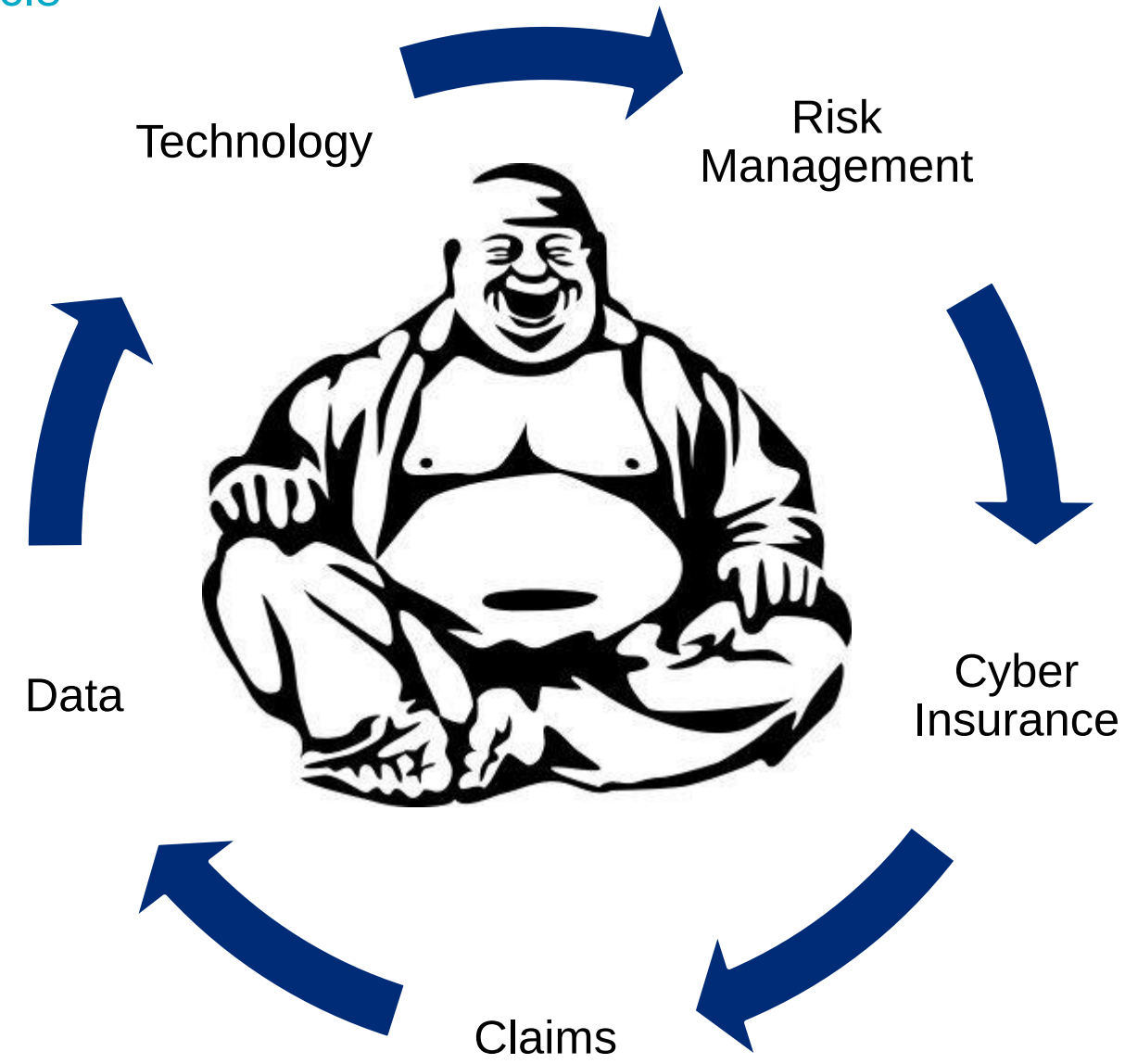
Source: PwC, Lloyds, BI Intelligence Estimates, 2015

2025 Vision


Clarity on
Fines
Silent cyber
is no more?
More Premium
More Claims Paid

2030 Vision

2030 Cyber Insurance Nirvana
Virtuous Cycle



Any Questions?