CONFIDENTIAL

The Limits of Risk Transfer
How a Reinsurer Assesses Crises

Autumn Seminar – Finnish Actuarial Society
17 November 2025

HOWDEN

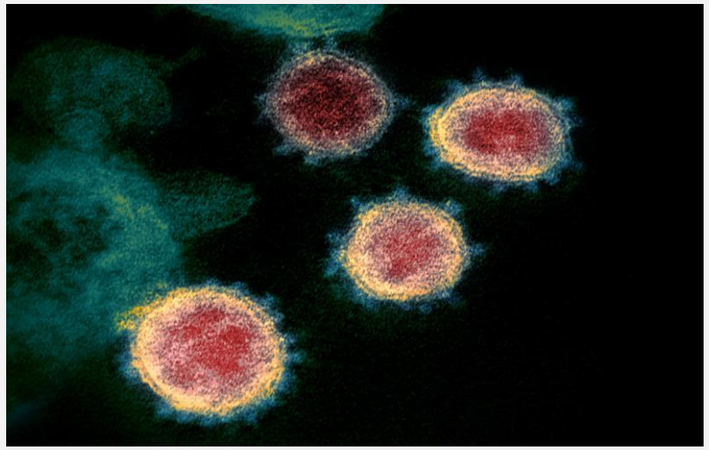
The Limits of Risk Transfer

Three core perils – three different market responses

Pandemic

Limited insurer appetite for pandemic cover and widely excluded

- Insurers offer some pandemic cover although usually at significant cost and limited to certain covers



Covid-19 – Insurance estimate $37bn*

Terrorism

Historical cover but severe dislocation following 9/11

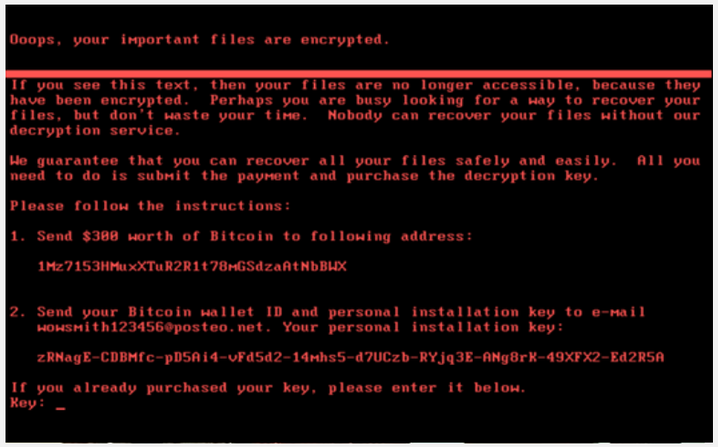
- Small commercial market with vast majority of exposure covered by pooling arrangements due to market dislocation post-9/11

September 11th - $60bn

Cyber

Fastest growing insurance line over last 5 years with ample capacity

- Market still growing although increasing unease at nation-state involvement in cyber attacks



NotPetya attack - $1.9bn

As the market grapples with the widening protection gap, identifying why some perils are covered and others not matters

Background – Relevance to the Topic

Mark Lynch – Head of Cyber Data and Analytics

Terrorism modelling – 2011-2017

- Lead the Impact Forecasting Terrorism and Political Violence modelling team at Aon for 5 years
- Lead analyst for Aon's engagements with pools (Pool Re, Extremus, Gareat, NHT, SASRIA)
- Developed Aon's computational fluid dynamic capabilities (blast modelling)
- MSc In Forensic Explosives and Explosive Investigation
- Part of the Life modelling working group (alongside Pandemic team)

Cyber modelling – 2018-2025

- Set up and built out Aon's cyber modelling capabilities internationally
- Built it from one team member to 15 analysts
- Led development of first IED, ILC and threat intelligence function
- Moved to Howden Re to as Head of Cyber Data and Analytics

Howden Re Cyber Team

Leadership

Luke Foord-Kelcey
Managing Director – Global Head of Cyber

Luke joined Howden Re in 2023, bringing over 20 years' experience of Cyber insurance and reinsurance broking & underwriting roles. Prior to joining Howden Re, Luke founded and led one of the largest Cyber reinsurance & retro broking teams. Before entering the insurance market, Luke was a lawyer in private practice at Barlow Lyde & Gilbert (now Clyde & Co).

Broking

Toby Lampier
Director – Head of Broking & Markets

Toby brings with him over 10 years of reinsurance treaty broking experience and an intimate knowledge of Cyber markets across rated carriers and ILS; broking the largest reinsurance and retrocessionary placements in the market. Toby was a founding member of the Aon Cyber reinsurance broking team, focusing on strategic and transactional Cyber reinsurance for a broad spectrum of clients globally.

Matthew Webb
Director – Head of Clients & Strategy

Matt spent the previous 18 years at Hiscox where he undertook a variety of underwriting roles including Group Head of Cyber and most recently as Line Underwriter for Cyber, setting up and growing their Lloyd's portfolio to over $80m GWP. During that time Matt Chaired the LMA Cyber Business Panel and led the project to develop the new LMA War exclusions.

Jack Sandford
Director – Senior Broker

Jack brings over 10 years' experience in the (re)insurance industry, with a background in Cyber analytics. Now working as a Cyber reinsurance broker, helping established clients leverage innovative products and analytics to optimise their treaty purchases, while working with new clients to help develop business plans to launch Cyber products and place appropriate reinsurance protection.

Patrick Bousfield
Managing Director – Senior Broker (Bermuda)

Paddy has 15 years' experience as a specialist insurance/reinsurance broker in a variety of markets, including Canada, London and the US. He has previously worked at Gallagher Re in London as an original member of the Cyber team, before founding the US Office.

Data, Analytics & Intelligence

Mark Lynch
Director – Head of Cyber Data & Analytics

Mark is leading our Cyber specific Data and Analytics function. A thought leader at the forefront of Cyber Exposure Management with 15 years' experience. Helping to build the first ILS collateralized Cyber placement, the first mono-line Cyber syndicate, bringing pension fund capacity to Cyber (re)insurers and is a highly skilled modeller, achieving optimal results for clients.

Cecilia Assmundson
Associate Director - Cyber Data & Analytics

Cecilia has over 7 years' experience in Cyber analytics and exposure management working previously at Aon and Chaucer. Cecilia has a deep understanding of the different model vendors and worked on modelling for a range of clients to support retrocession & reinsurance placements. She has been driving the development CyberNova; our proprietary Industry Exposure Databased (IED).

Harriet Gruen
Director – Head of Threat Intelligence

Harriet is the Head of Cyber Threat Intelligence at Howden Re, building insurance focused threat intelligence products. Harriet has systemic risk modelling and threat intelligence experience in the insurance and financial services industry, including at AXIS Capital, Tokio Marine Group and HSBC. She is currently a European Cybersecurity Fellow as part of the European Cyber Conflict Research Initiative (ECCRI) and holds a CISSP certification. Harriet has an MSc from the London School of Economics..

Ioannis Spanos
Associate - Cyber Actuary

Ioannis joined Howden as a Cyber Actuary in 2024, bringing a robust foundation in Mathematics, Statistics, and Data Science. He recently earned a Master's degree in Statistics and Data Science from Imperial College London, where he specialized in areas such as Machine Learning, Deep Learning, and Survival Models. His thesis focused on Extreme Value Modelling with Missing Data, showcasing his expertise in tackling complex statistical challenges.

Senior resource with Cyber expertise

Josh Everdell
Managing Director
– Global Head of Casualty

Steve Hanke
Managing Director
– Broker (US)

Ken Kim
Managing Director
– Broker (US)

Carrie Byler
Managing Director
– US Head of Casualty

Wolfram Schultz
Head of Casualty & Cyber
– Continental Europe

Anke Salm
Managing Director
– Broker (Europe)

Craig McCoig-Lees
Director
– Broker (Singapore)

Adam Matteson
Director
– Broker (Australia)

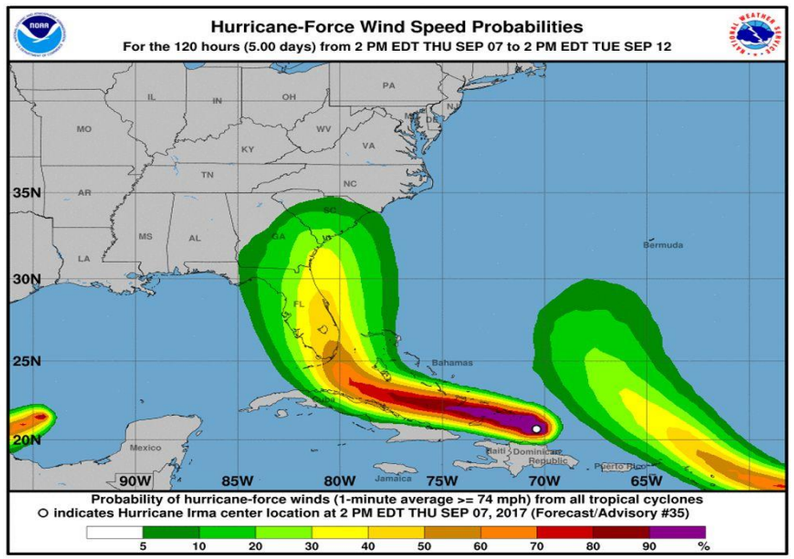
Key criteria for reinsurers when assessing this risk

01. Event Footprinting
02. Historical Catalogue and Anchoring
03. Data Limitations
04. Severity Modelling and Known Unknowns
05. State-sponsored activity
06. Pooling arrangements
07. Implications for Cyber

1. Event footprinting

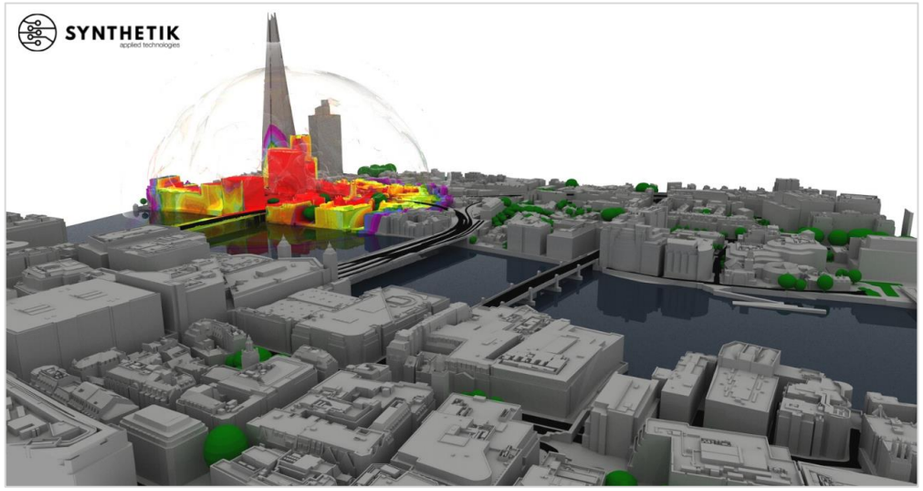
Geographical diversification key for aggregation control

Within the natural perils geography is king and even without sophisticated modelling simple footprinting can give you a good understanding of loss ramifications



As a base principle if you (re)insurer properties in Florida (hurricane risk), California (earthquake) and Minnesota (winter storms) then you should diversify away from one peril

However, some events, like Irma (modelled) were potentially large enough to dislocate the entire market



Within terrorism modelling geography is even more important as the typical radius of blasts is small (<250m)

As a result, significant time and effort has been made to move the market from a concentric circle approach (upper graph) to a shift towards computational fluid dynamics (lower exhibit)

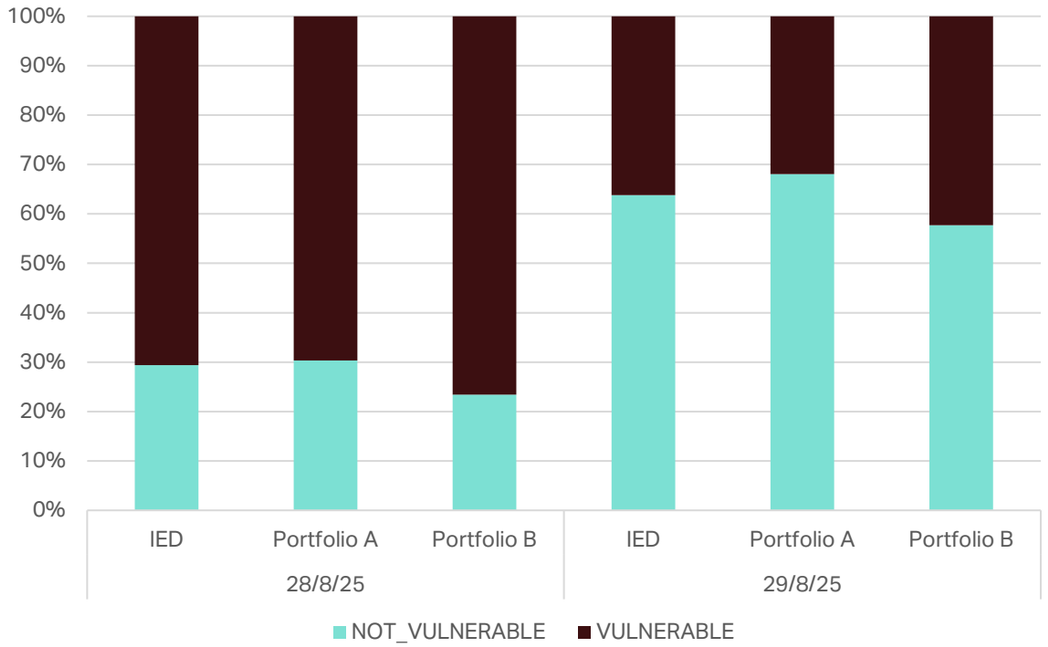
This allows insurers to get a bespoke footprint for a blast taking into consideration building density, street networking and construction.

Sources: NHC, Synthetik, Royal Holloway

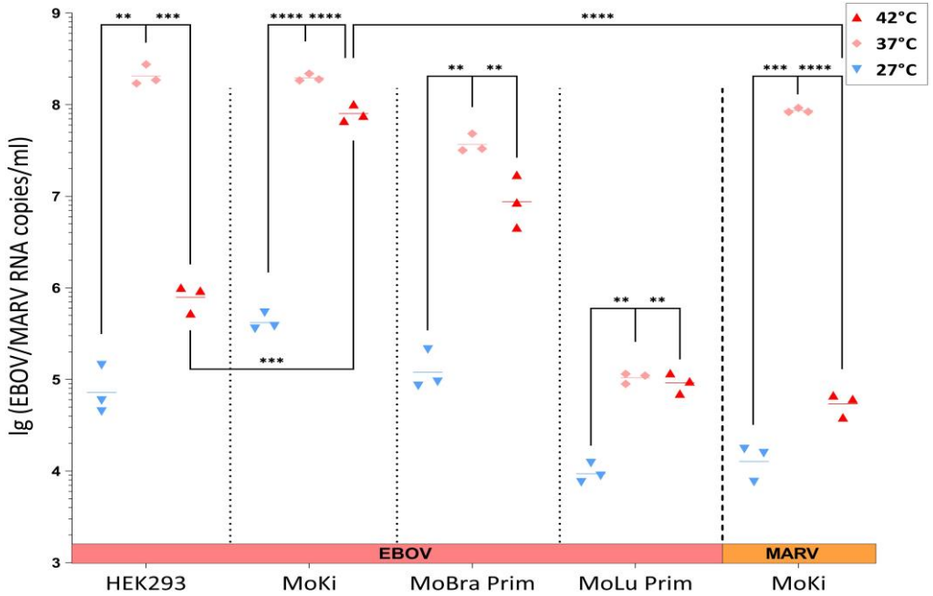
1. Event footprinting

What do you do if physical geography is less relevant?

Cyber modelling – Remediation Rate CVE-2025-7775 Citrix NetScaler



Pandemic modelling – Replication rate of ebola in differing ambient temperatures



Cyber modelling – Mapping technology

For cyber the central emphasis is mapping technology stacks (who uses what software) and vulnerabilities (who has exposure to a particular threat). This is usually done through outside-in scanning and underwriter questionnaires

Pandemic modelling – Mapping replication conditions

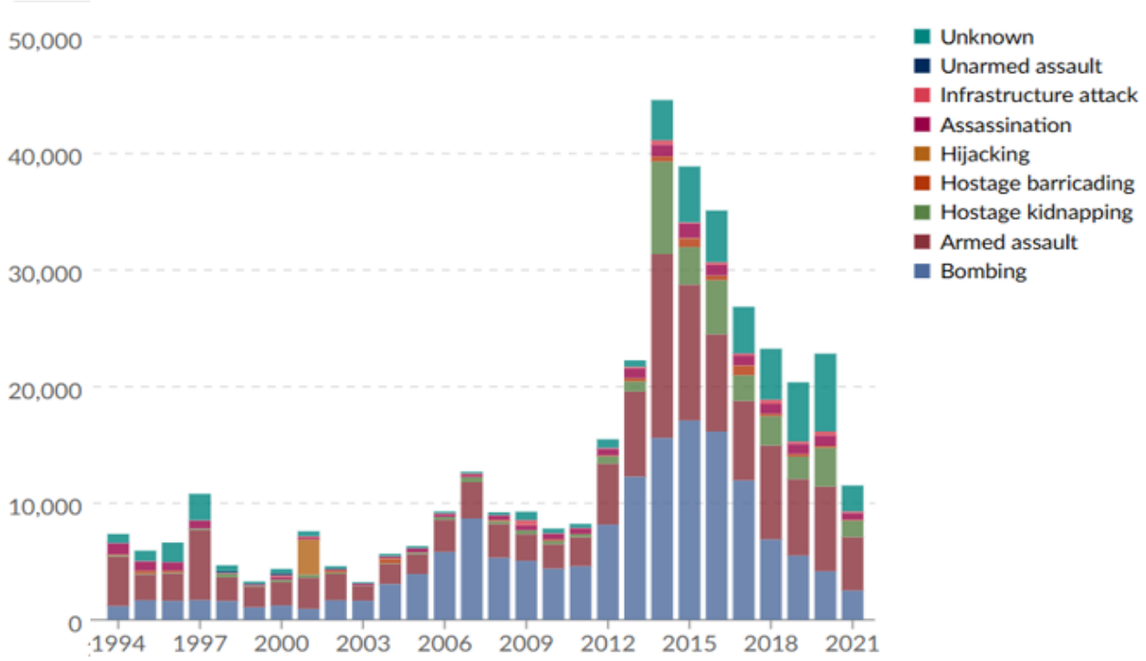
For pandemic modelling, the only real way to build a model of potential impact is to model the conditions for each viral strain. This means that the number of permutations will dramatically outstrip the means available to the insurance industry

Sources: Howden analysis of our industry exposure database, Bokelmen et al.

2. Historical Catalogue and Anchoring
Limitations and Impact on Market Development

Problem 1 – Terrorism modelling (anchoring)

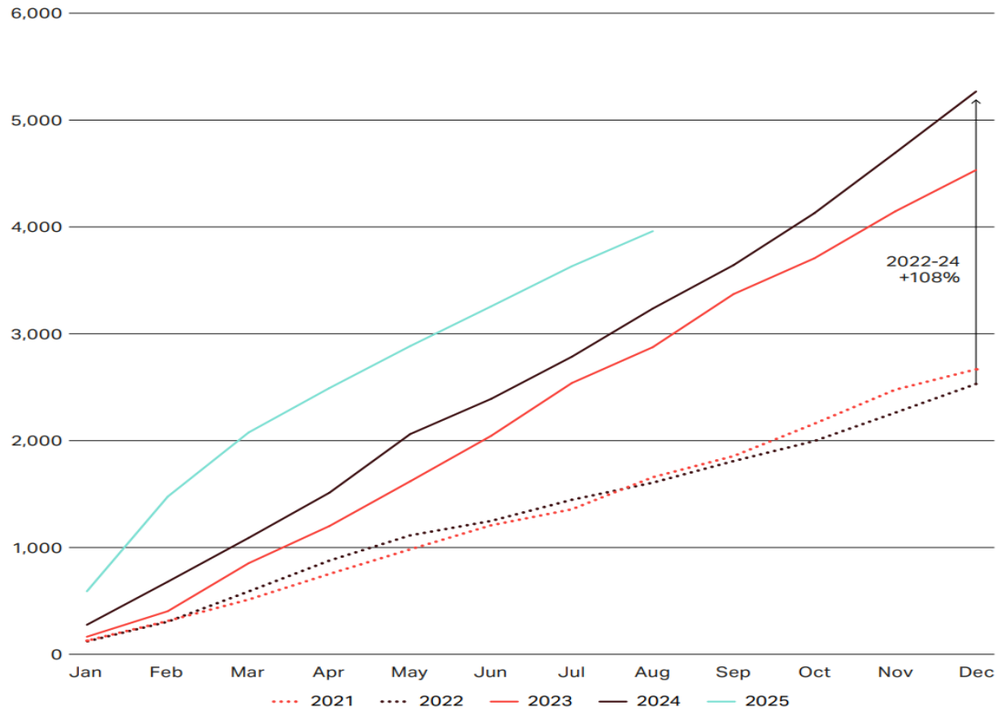
Despite hijacking being a small overall component of the global incidences of terrorism since the mid-90s anchoring bias towards 9/11 mean it has a disproportionate impact on the market



Source: Global Terrorism Database

Problem 2 – Cyber modelling (extrapolation)

Cyber incidents have being going up materially in the last 2-3 years however these have been attritional events led by criminal gangs. These events are seen by most security experts as independent of catastrophic potential



Source: Howden analysis of NCC data

2. Historical Catalogue and Anchoring
Implications for probabilistic modelling

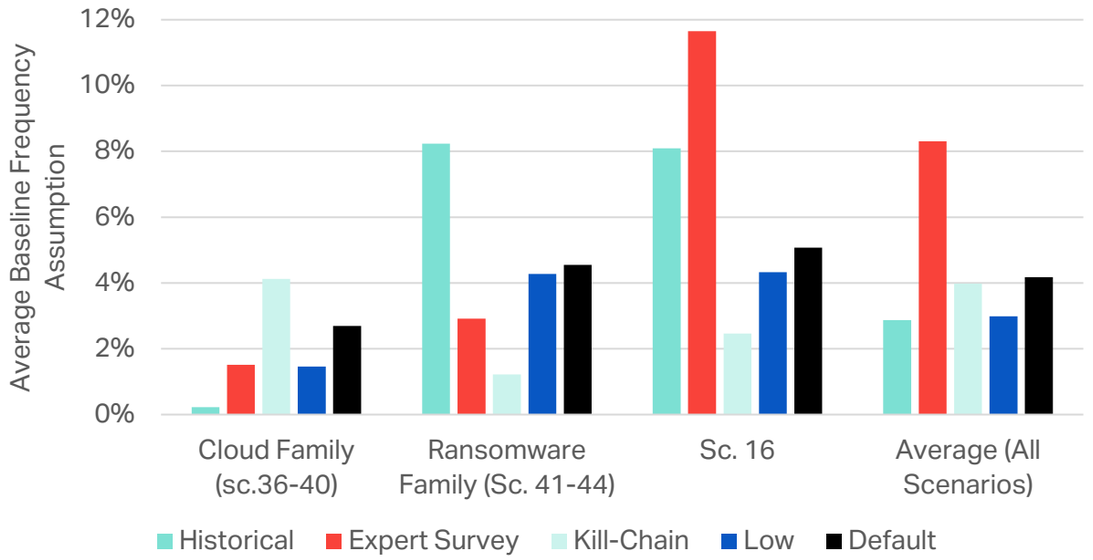
Overfitting the historical catalogue

Without specific knowledge of a country's geopolitical history can lead to insurers to extrapolate from historical incidents that are no longer relevant. For example, the significant volume of bombings in the 1980s and 1990s in the UK is irrelevant for forward looking projections for 2026

The Baltic exchange bombings by the IRA actually facilitated the UK setting up one of the first terrorism pools (Pool Re)

Overreliance on expert survey questionnaires

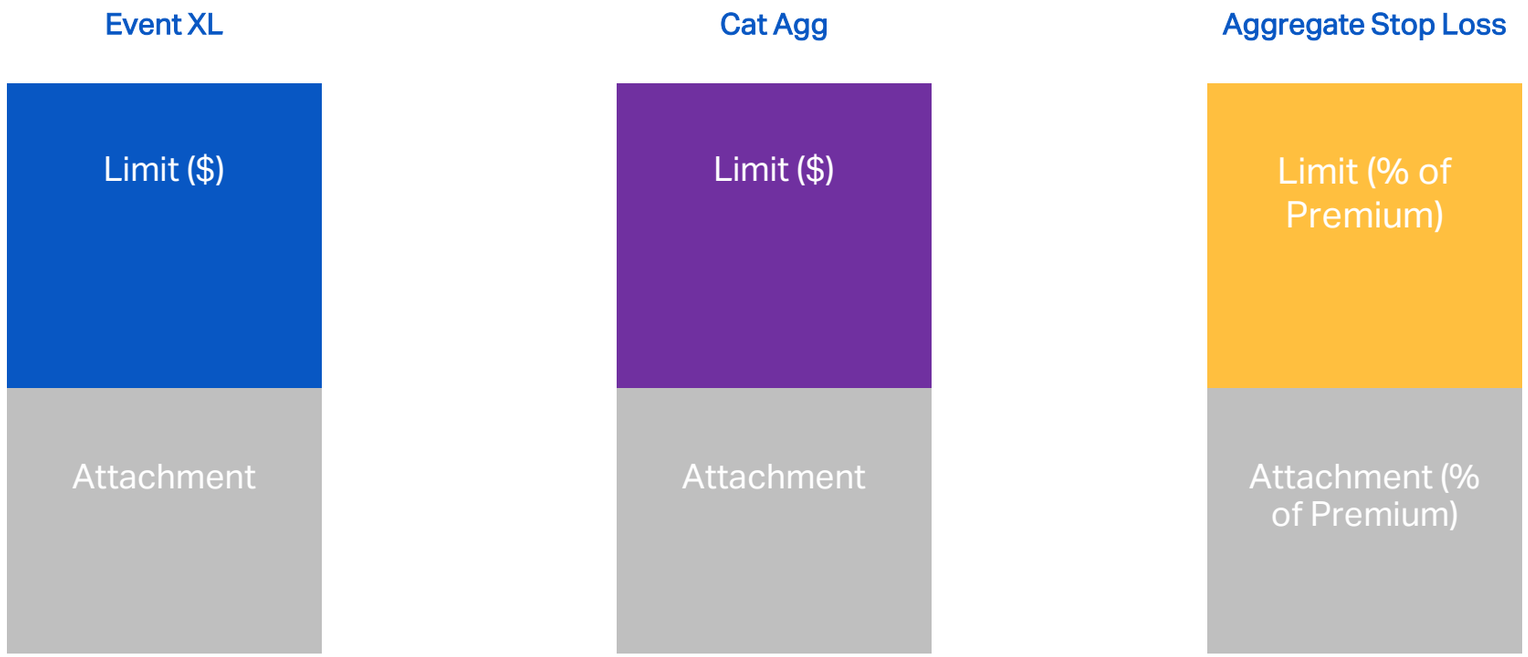
For perils like cyber and pandemic (and CBRN terrorism) where there are no historical precedents then there is a heavy reliance on expert survey data. There is a large body of academic literature that suggests that subject matter experts are still prone to catastrophising and recency bias



Source: Howden analysis of CyberCube Event Rates

2. Using Structuring to Mitigate Risk

If severity is better understood than frequency this influences what is offered



	Event XL	Cat Agg	Stop Loss
Multiple Events Covered	No	Yes	Yes
Catastrophe & Attrition	Cat Only	Cat Only	Cat and Attrition
Reinstatements	Yes (additional cost	No	No

3. Data Limitations

Quality of client data may undermine modelling efforts

Pandemic

Key Areas of Focus

- Event cancellation – standardisation of data capture for this peril key for continued support for this class
- Non-damage BI costs – these are vary rarely if ever codified into an EDM format, that needs to change
- Life data – age profile and pre-existing conditions vital for modelling, living conditions (multi-generational households) vital as well
- Geographic information – in territories where there are state or municipality level decisions on preventative measures this needs captured

Terrorism

Key Areas of Focus

- Geolocation data – this has to be at lat/lon level at worst. Postal or above leads to skewed concentrations
- Building construction – significant impact on severity in particular projectiles from fragments
- Elevation data (life) – If employees are on upper floors they may be shielded form major effects of explosives
- Time of day (life) – knowing the work to home transition helps (re)insurers model concentrations depending on time of day

Cyber

Key Areas of Focus

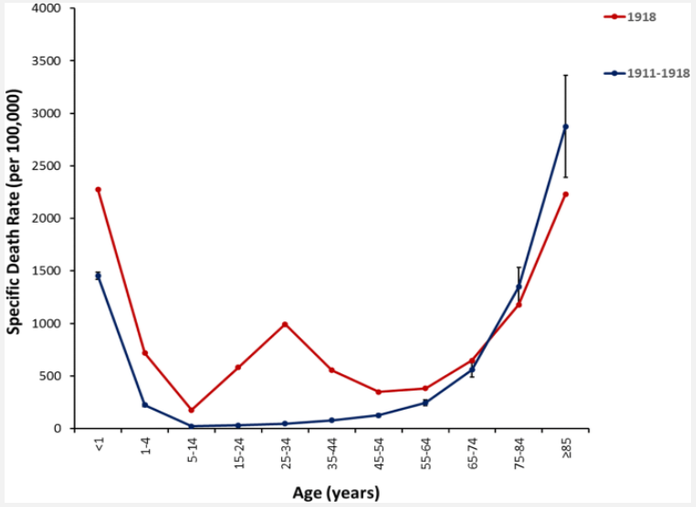
- Revenue and industry classification – base assumptions in cyber models use these two variables if they are incorrect this will skew results
- Parent/subsidiary flags – knowing if you are talking about Toyota group or a subsidiary of Toyota in Finland makes a huge difference
- Secondary modifiers – security controls such as patching and network segmentation can materially change losses but this isn't always flagged

4. Severity Modelling
Varying degrees of knowledge

Pandemic

Gaps between incidents raises challenges

- Prior to the COVID-19 pandemic most pandemic models were relatively rudimentary and used prior events such as SARS of Spanish flu (shown below) to model severity
- Like Earthquake modelling the gaps between events mean that there is a high degree of uncertainty in severity modelling

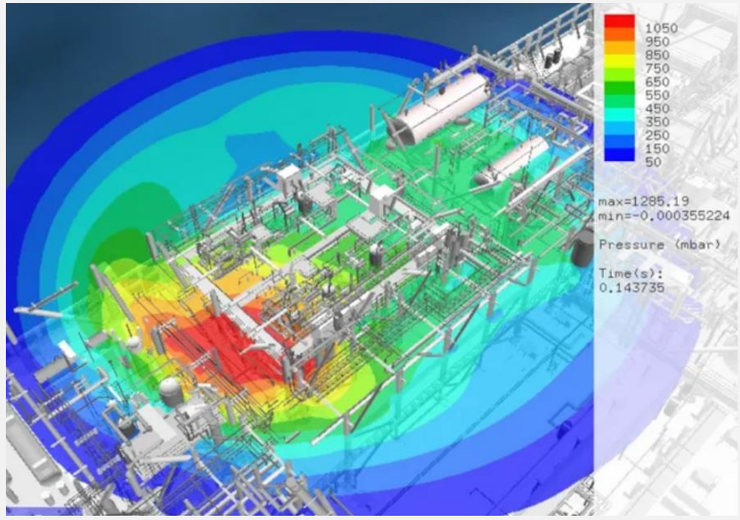


Source: Taubenberger and Morens (2006)

Terrorism

Military testing makes severity more certain

- Due to the significant volume of military testing of explosives and CBRN agents knowledge about the impact of explosives is well understood
- This means that (where required) terrorism modelling can be incredibly accurate



Source: EXSIM CFD Software

Cyber

Extrapolation from standalone claims

- As there has been a high level of cyber claims for standalone cyber incidents there is significant data to extrapolate severity to the wider market
- What isn't known is what the implications are for phenomena such as demand surge of "hive mind" security

Source: Marcus Hutchins.com

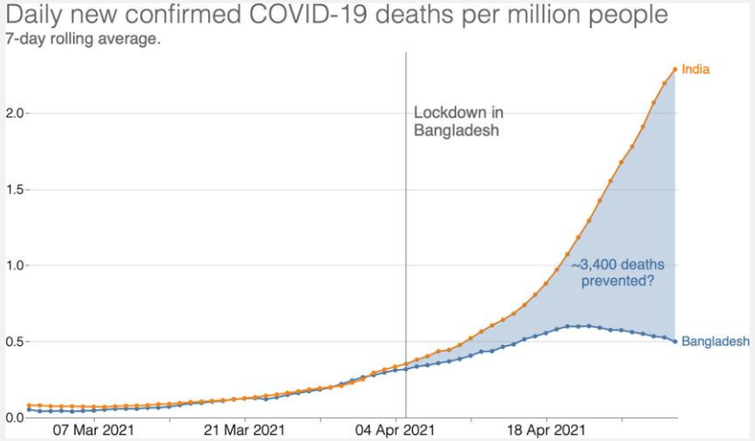
4. Known Unknowns

Core assumptions that have not been stress tested

Pandemic

Political appetite for further lockdowns

- Public appetite for further lockdowns or protection measures will differ from country to country and will be based on the political climate
- Significant implications for the severity of loss which is decided in the middle of an event's trajectory

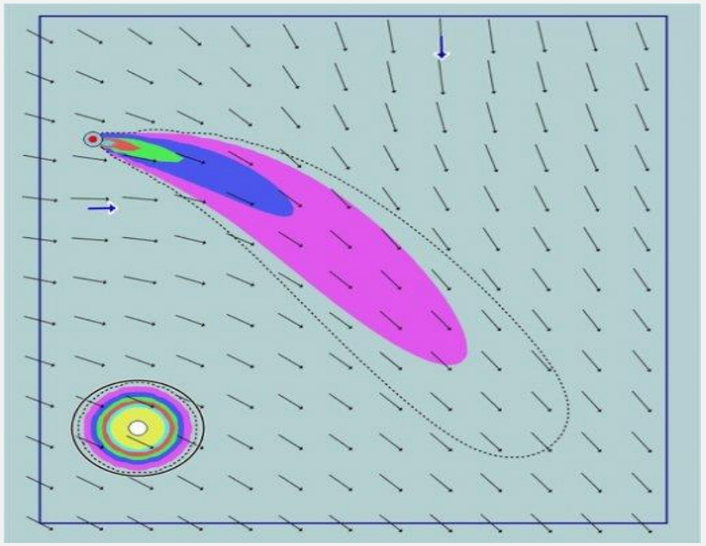


Source: Sawant (2023)

Terrorism

Decontamination for CBRN events

- The responsibility for decontamination post-event is vague in a number of countries.
- In most circumstances, the decontamination costs would be higher than any PD costs



Source: ALOHA (DHS software)

Cyber

Reliance on cloud

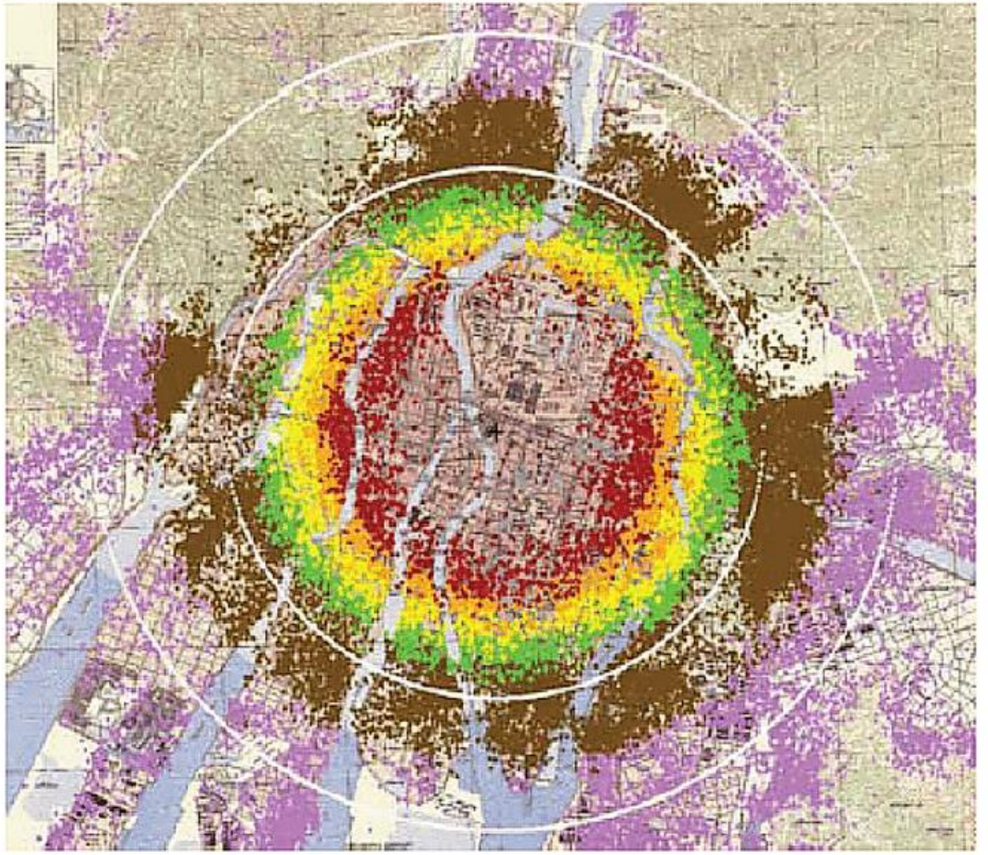
- While it is possible to identify who is using what cloud system its much harder to identify what they are using it for
- Outages to AWS, Google Cloud and Microsoft Azure have not been long enough to test this

	Small	*Medium*	*Large*
Healthcare	49.0%	45.5%	31.1%
Financials	58.7%	54.0%	34.9%
Banking	49.0%	45.5%	31.1%
Retail	39.3%	36.9%	27.2%
Manufacturing	39.3%	36.9%	27.2%
Energy & Utilities	39.3%	36.9%	27.2%
Oil & Gas	20.0%	19.9%	19.5%
Aviation	39.3%	36.9%	27.2%
Marine	19.8%	19.2%	16.5%
Information Technology	58.7%	54.0%	34.9%
Agriculture	20.0%	19.9%	19.5%

Source: Lloyds Cloud Cascade Template

5. State Sponsored Activity

Limited interest from insurers in state-level machinations



Nuclear exclusions common in terrorism

Market expectation remains that any nuclear attack would have to have element of state-sponsored behaviour and should be excluded

Clause	Key Features	Exclusion/Limitations	Attribution Requirements
LMA 5564A	Excludes losses directly or indirectly arising from war and/or cyber operations.	Excludes any cyber operations that disrupt, deny access to, or degrade computer systems or manipulate/destroy information. Excludes both direct and indirect losses related to state-backed operations.	Requires objective evidence for attribution, such as formal or official attribution by the affected state's government.
LMA 5564B	Similar to 5564A but with broader and less stringent attribution requirements.	Still excludes losses from significant state-affecting cyber operations but allows more flexibility in applying exclusions.	Attribution is less strict compared to LMA 5564A, allowing more flexibility in determining state responsibility.
LMA 5565A	Focuses on cyber operations linked to war or that significantly impair a state's essential services or security.	Excludes cyber operations that are part of or in preparation for war, as well as any operation that causes a state to become an "impacted state." Limits for other cyber operations must be specified, or they are not covered.	Requires objective evidence for attribution, including formal declarations by the affected state.
LMA 5565B	Mirrors LMA 5565A but with fewer stringent exclusion limits for cyber operations not directly linked to war.	Allows more flexibility for covering cyber operations not directly tied to war but still excludes major systemic events that impair a state's ability to function.	Less rigid attribution process, allowing parties to agree on evidence.
LMA 5566A	Broad exclusion of cyber operations that significantly impair essential services or the security of a state, with special attention to war preparation.	Excludes cyber operations that cause a state to become an impacted state, defined as causing major disruption to essential services like financial systems or defense.	Similar attribution requirements, requiring evidence from governments or official sources.
LMA 5566B	Similar to LMA 5566A but with a broader scope that allows for some exceptions based on location of the computer systems impacted.	Excludes cyber operations but allows coverage for computer systems not located in the impacted state but affected by the cyber operation.	Similar attribution process to LMA 5566A.
LMA 5567A	Introduces an exception for cyber operations impacting systems not physically located in the affected state.	Excludes cyber operations that affect states directly, but allows for coverage when the insured's systems or third-party systems are not physically located in the impacted state.	Requires attribution based on objective evidence from governments or recognized entities.
LMA 5567B	Mirrors LMA 5567A but with more specific attention to defining essential services and state-level impacts.	Excludes cyber operations causing major detrimental impacts to essential state services or defense, but allows coverage for systems located outside the impacted state.	Requires clear evidence of state involvement, including formal attribution.

Cyber war exclusions (significant market debate)

Following the Ukraine invasion in 2022 reinsurers strongly influenced the market into adopting cyber war exclusions to protect against significant nation-state activity. This is still highly controversial (particularly outside Lloyds)

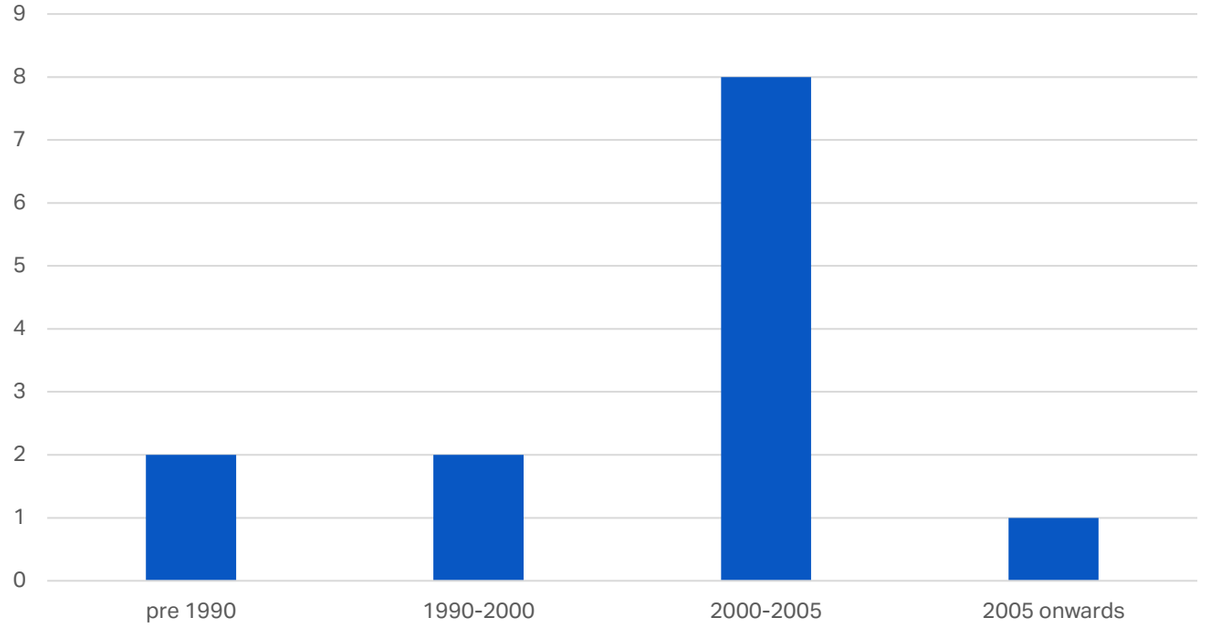
Source: Japanese Department of Health, Pinnacle One

6. Pooling Arrangements

What can be learned from Terrorism Pools?

Country / Pool	Buys Reinsurance	Government Backstop	Cyber / Pandemic under consideration
Australia	Yes	Yes	No
Austria	Yes	No	No
Belgium	Yes	Yes	No
Denmark	No	Yes	No
France	Yes	Yes	No
Germany	Yes	Yes	Yes
India	Yes	No	No
Israel	No	Yes	No
Netherlands	Yes	No	No
South Africa	Yes	No	No
Spain	No	Yes	Cyber (if terrorism)
United Kingdom	Yes	Yes	Yes (cyber PD)
United States	No	Yes	No

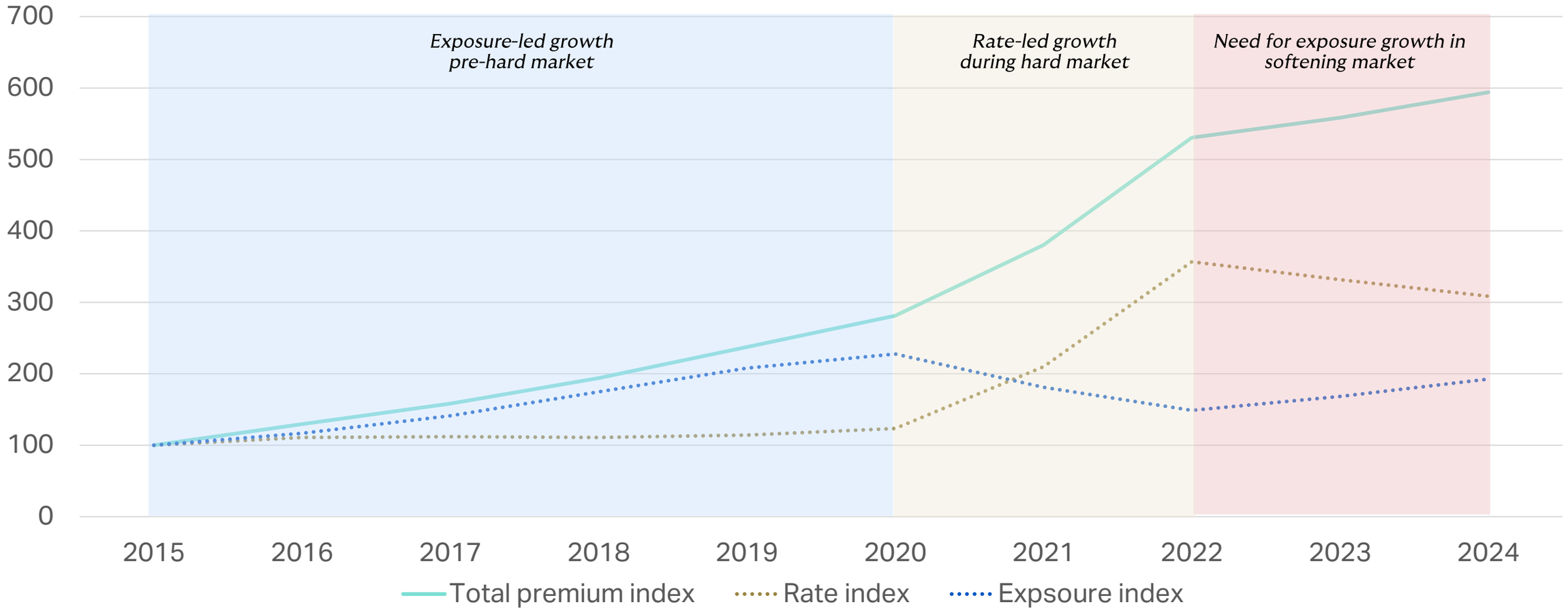
Clear impact of September 11 leading to government intervention



pre 1990	1990-2000	2000-2005	2005 onwards
Israel (1941)	United Kingdom (1993)	Austria (2002)	Belgium (2008)
South Africa (1979)	Spain (1995*)	France (2002)	
		Germany (2002)	
		India (2002)	
		United States (2002)	
		Australia (2003)	
		Netherlands (2003)	
		Denmark (2005)	

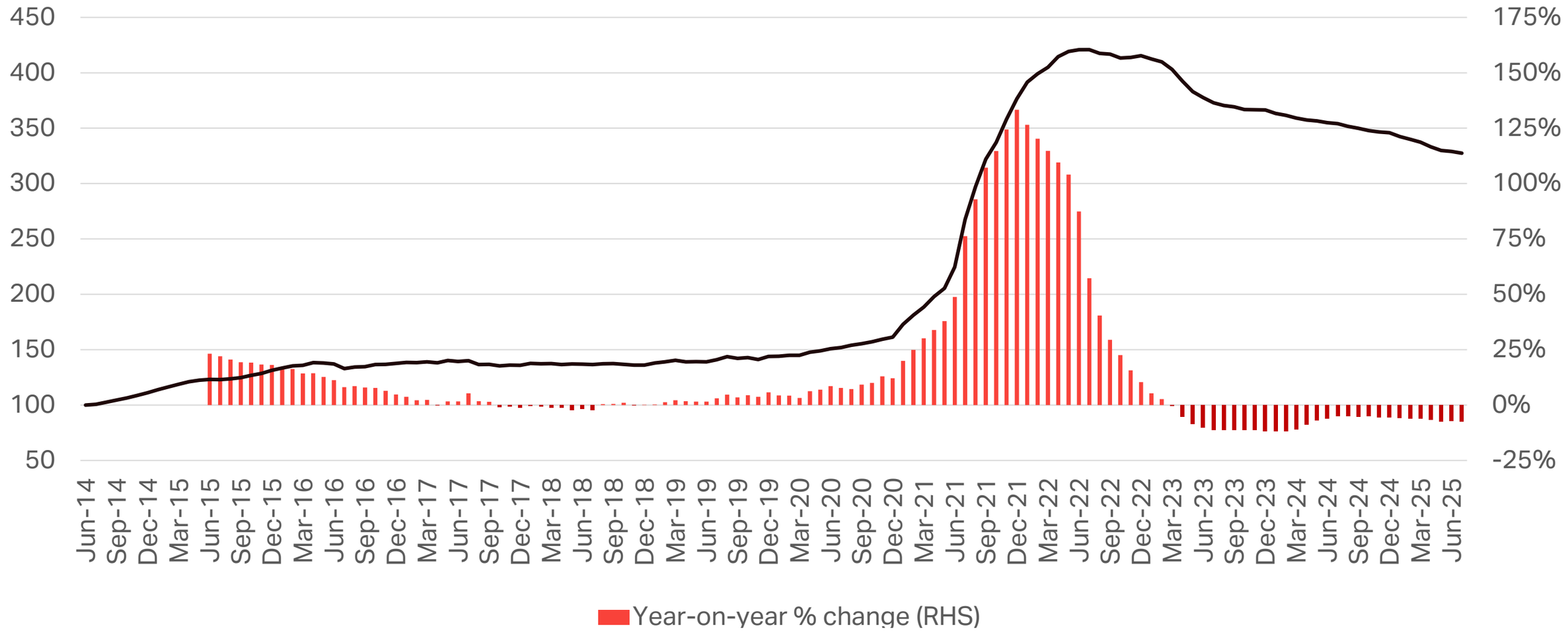
7. Implications for Cyber

Premium growth continues despite some slowing



7. Implications for Cyber

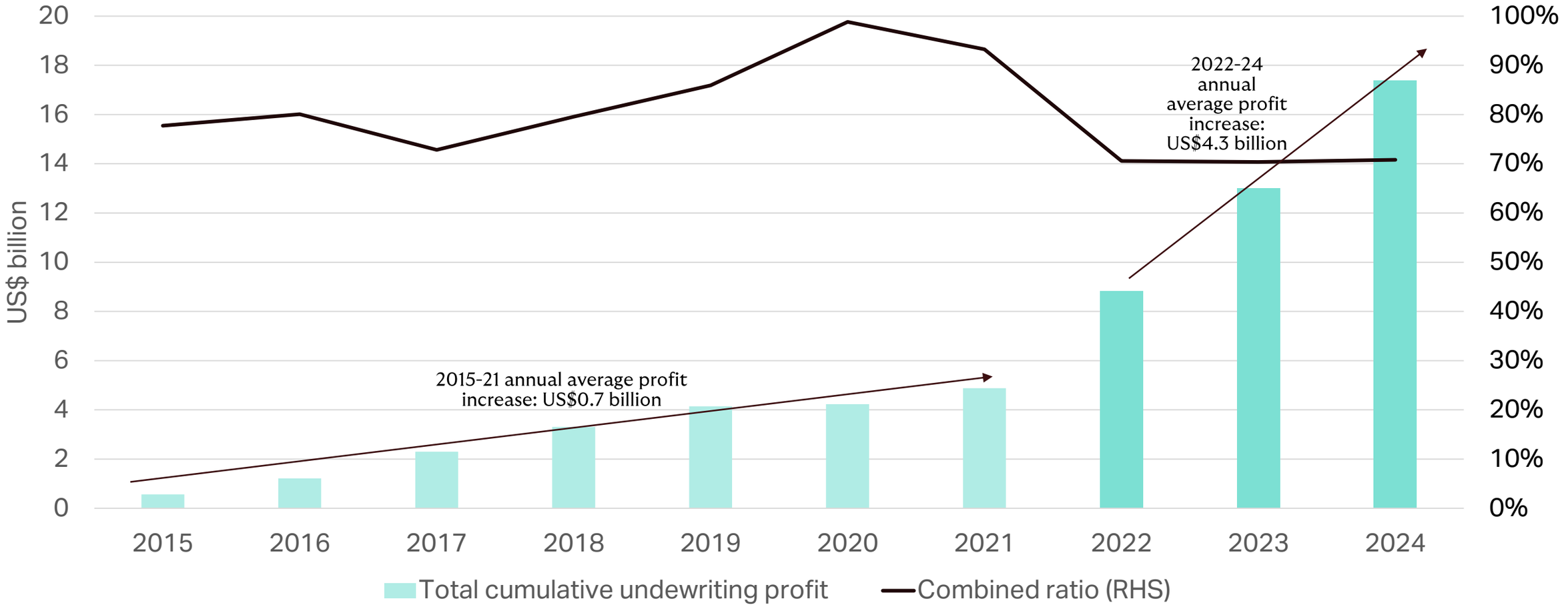
Rate volatility still evident which may lead to a shock post -cat



7. Implications for Cyber

(Re)Insurers still seeing material profitability

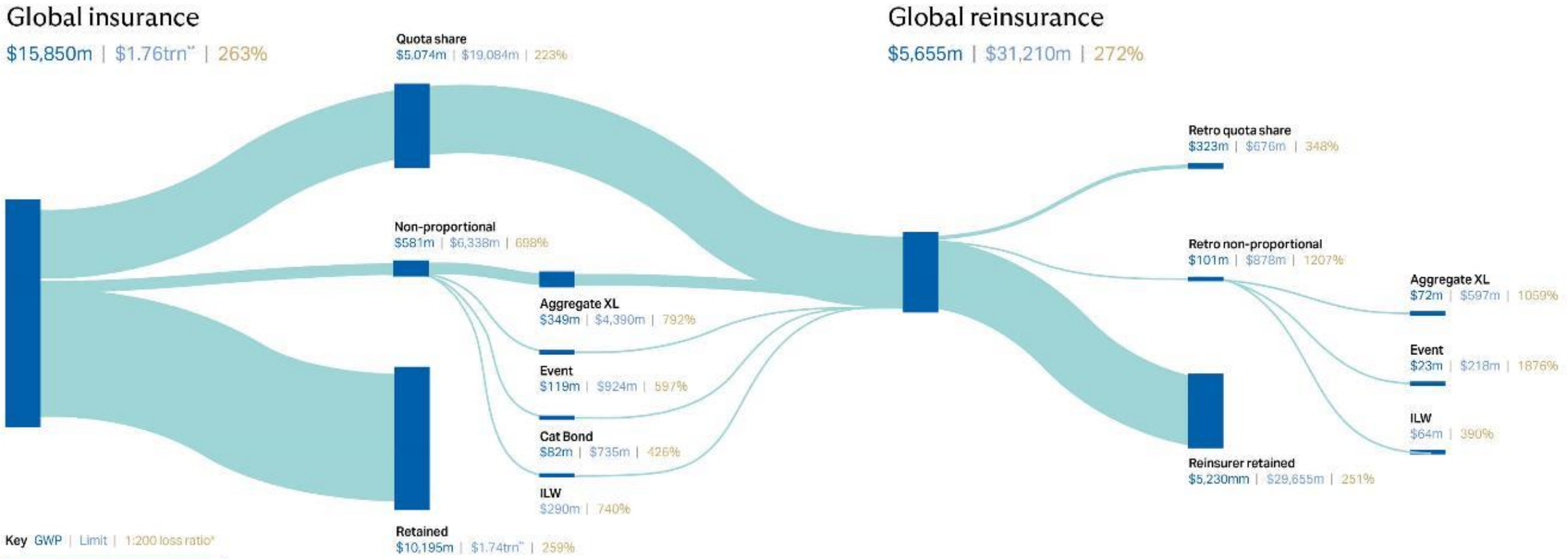
Cumulative underwriting profit global cyber insurance market – 2015 to 2024



Note: Global market based on premium and loss ratio data from Howden and third parties, including NAIC, Lloyd's and Beazley. Source: Howden

Global Cyber Market 2025: Insurance, Reinsurance & Retro

Premium flows across the cyber (re)insurance market



*Loss ratio at AEP 200yr return period for gross of acquisition costs

** Excludes some endorsement/embedded business which represents a very small proportion of overall premium

36%
of GWP ceded to reinsurers

$5bn
Size of reinsurance QS market (in GWP)

$581m
Size of reinsurance non-proportional market (in GWP)

7%
Retrocession utilisation (% of reinsurer GWP)

Conclusions

a. Significant modelling challenges exist for all three perils that make them difficult to (re)insure
b. Market dislocation significantly more likely post-catastrophe (9/11, COVID-19) which leads to pooling or simply omission
c. This is amplified if there are limited additional data points to contextualise that event
d. Cyber market differs from the others by being in the honeymoon phase prior to a major event taking place
e. The ability to build up a large premium base and profitability might shelter the cyber market from the worst overreactions
f. Cyber reinsurance is highly concentrated (80% with top 10 reinsurers) so movements by one or more can sway the market significantly

Proximity to a large catastrophe is the strongest indicator for market dislocation but cyber may be able to learn from this

Howden Re
One Creechurch Place, London EC3A 5AF

T: +44 (0) 20 7398 4888
E: howdenreinfo@howdenRe.com

www.howdenre.com