THE GENEVA ASSOCIATION

INSURANCE FOR A BETTER WORLD

CATALYSING CYBER RISK TRANSFER TO CAPITAL MARKETS:
Catastrophe bonds and beyond

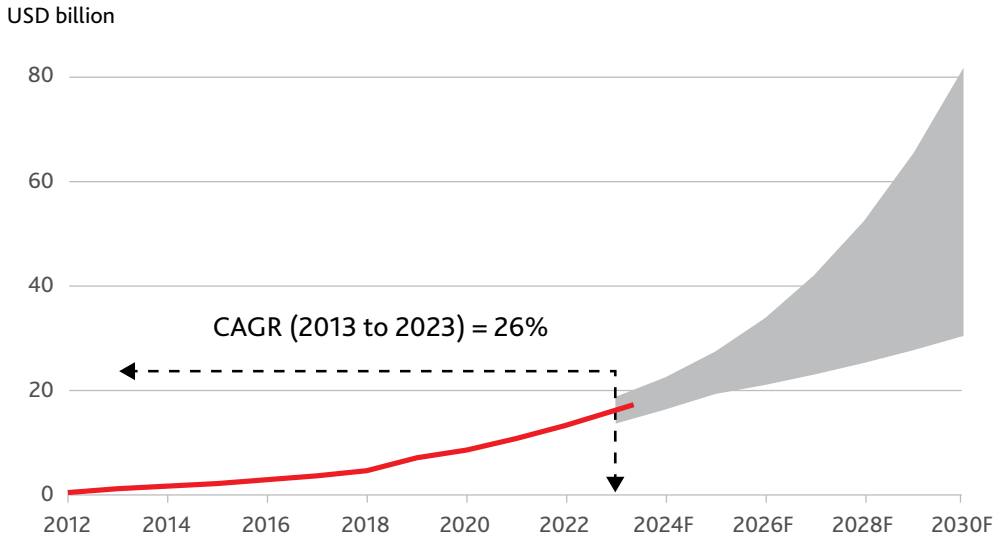
Research summary | December 2024

Darren Pain, Director Cyber | Evolving Liability, Geneva Association

Against the background of sharply rising cyber risk exposures, dedicated cyber insurance has developed rapidly, providing not only funds to repair and recover affected data and systems following an incident, but through its underwriting procedures encouraging insureds to invest in best practice cyber hygiene. Global premiums for cyber insurance have increased sharply from less than USD 1.5 billion in 2013 to around USD 15 billion in 2023, albeit this still represents less than 1% of the total P&C insurance market.[1] The scope of coverage has also broadened to include a range of cyber-related losses such as costs for data recovery, IT forensics and system restoration, non-damage business interruption as well as liabilities for damages incurred by third parties.

As societies continue to digitalise, most industry commentators anticipate further strong upward momentum in the cyber insurance market. That reflects an anticipated increased take-up of cyber insurance across sectors and countries, as firms' and individuals' awareness of cyber risk rises and recognition of their degree of underinsurance grows. In this way, cyber insurance can play an increasingly important role in helping to narrow what is a large and persistent protection gap.

FIGURE 1: CYBER INSURANCE MARKET OUTLOOK – GLOBAL PREMIUM PROJECTIONS



Notes: The red line shows global cyber insurance premiums up to 2023 according to Howden. The shaded band shows the range of premium forecasts from the following market participants and commentators: Beazley, Business Research Company, Cognitive Market Research, Expert Market Research, Fortune Business Insights, Global Market Insights, Howden, Market.us, Morningstar DBRS, Munich Re, S&P, SkyQuest Technology, Spherical Insights and QualRisk. Where the forecast horizons differ, the data are projected using the implied compound growth rate.

CAGR = compound annual growth rate

Source: Howden and Geneva Association calculations

1 Howden 2024; Allianz 2024.

However, realising such continued rapid growth in cyber insurance will depend crucially on attracting sufficient capital to back the underlying policies. Reinsurance, in particular, is vital for primary insurers to lay off peak cyber risks, which otherwise would strain their balance sheets. Estimates vary from year to year and across countries, but primary insurers probably cede around 50% of their cyber premiums to reinsurers, far more than other lines of insurance.[2]

Alternative risk-absorbing capital

Alongside broadening traditional re/insurance participation in underwriting cyber risks, tapping additional risk-bearing capital from outside the sector will likely be essential. The size of possible extreme cyber losses is too large and/or uncertain for re/insurers to carry alone. One recent study suggests a five-fold increase in capital will be required to sustain even the more conservative market projections for cyber insurance premium growth.[3] This includes transferring some cyber exposures to financial markets, where the pool of potential capital to invest in emerging risks like cyber is much deeper.

The prospect of cyber insurance linked securities (ILS) – financial instruments that bundle together specific insurance risks into a distinct investable asset – has been talked about for years. While a few private cyber collateralised reinsurance and sidecar agreements have been transacted from around 2017, these were sporadic, involving a few selected participants. Recently, however, cyber ILS issuance has accelerated with several notable deals coming to market. For example, since the start of 2023 at least five different re/insurers have issued cyber ILS (Table 1). This includes the first fully securitised cyber Cat bonds (a security that reimburses claims arising from a major cyber incident should they exceed some pre-agreed threshold).

TABLE 1: RECENT CYBER ILS TRANSACTIONS

Date of issuance	Sponsor (SPI)	Coverage limit (USD mn)	Transaction type	Maturity	Trigger type (basis)
Jan 2023	Hannover Re	100	Collateralised reinsurance	Unknown	lndemnity (quota share)
Jan–Sep 2023	Beazley (Cairney)	71.S (over three tranches)	Prívate cat bond (Reg4(a)(2) format)	One year (matured Jan 2024)	lndemnity (per occurrence)
Nov 2023	AXIS (Long Walk Re)	75	Cat bond (144A format)	Two years	lndemnity (per occurrence)
Dec 2023	Chubb (East Lane Re VII)	150	Cat bond (144A format)	Two years	lndemnity (per occurrence)
Dec 2023	Beazley (PoleStar Re)	140	Cat bond (144A format)	Two years	lndemnity (per occurrence)
Dec 2023	Swiss Re (Matterhorn Re)	so	Cat bond (144A format)	Two years	PERILS industry loss (per occurrence)
Jan 2024	Swiss Re	so	ILW	Unknown	PERILS industry loss (per occurrence)
Apr 2024	HannoverRe (Cumulus Re)	13.75	Prívate cat bond (Reg 4(a)(2) format)	One year	Parametric (outage duration of major US cloud provider regions)
May 2024	Beazley (PoleStar Re)	160	Cat bond (144A format)	Two and a half years	lndemnity (per occurrence)
Sep 2024	Beazley (PoleStar Re)	210	Cat bond (144A format)	Three years	lndemnity (per occurrence)

Source: Geneva Association based on published sources

2 Cited in Risk & Insurance 2024. While cyber cession rates in the latest reinsurance renewals suggest an average in the 40s – see Gallagher Re 2024 – this still compares with 10% to 15% for more mature insurance lines such as property and liability, as reported in American Academy of Actuaries 2021.

3 Specifically, risk carriers will reportedly need USD 121 billion of capital to manage a 1-in-250 year loss on U.S. cyber insurance policies, a 500% increase on the current estimated capital base. See CyberCube 2024.

Although the amount of transferred cyber risk via these bonds (around USD 800 million) remains modest, both in absolute terms and relative to the re/insurance sector's aggregate cyber exposure limit, the transactions nonetheless mark an important milestone in the development of the cyber re/insurance market.[4] A key issue is whether market conditions are ripe for a significant and sustained upscaling in cyber risk transfer to capital markets, a crucial future step in distributing catastrophic cyber exposures to those most willing and able to absorb them.

Market intelligence on recent cyber Cat bonds

Discussions with market participants highlighted several design features that were prominent in negotiations between sponsors and third-party investors of the recently issued cyber Cat bonds. First, there has been a pivot in favour of tradable securities, especially those with a Rule 144A format that streamline the placement process and widen the resale opportunities for sophisticated investors. Second, ILS investors typically want exposure to extreme but rare cyber risks meaning that most of the recent cyber ILS have been structured as per occurrence, excess-of-loss coverage that pay out if the loss from a single major cyber event exceeds a given threshold. Third, pricing on the initial cyber Cat bonds suggests the compensation required by third-party investors for taking on extreme cyber exposure is larger than for other Nat Cat perils, in part at least linked to the uncertainty often attached to a new and unfamiliar investment product.

Reducing the cost of ILS-sourced capital will be crucial if the terms of risk exchange are to become more viable for sponsors of larger and regular programmes of cyber ILS. More generally, the initial cyber ILS transactions revealed some important underlying challenges. Most notably:

- Varied definitions of events that trigger insurance payouts (i.e. the perils included, temporal limits, damages covered etc.) and different language for policy exclusions (e.g. for war, critical infrastructure) potentially undermine contract certainty.
- The primary investor base in cyber is still narrow (although expanding) while limited secondary market trading means ILS as an asset class is relatively illiquid.
- Investors remain cautious about the potential diversification benefits cyber risks offer their portfolios, given the potential for incidents to impact many companies simultaneously and reduce the prices of a wide array of financial assets.

Overall, virtually all interviewees – sponsors, investors and intermediaries – perceive a cyber ILS market still in development rather than on the verge of lift-off. While the recent deals helped lay important groundwork, not least educating investors about cyber risks and associated loss modelling, the most likely outlook is for continued, steady expansion rather than rapid acceleration in future issuance.[5] The investor base remains small and opportunistic, and the current high capital and transaction costs likely prohibit routine transfer of peak cyber risks to capital markets.

Promoting cyber risk transfer to capital markets

Some of these headwinds will no doubt subside as overall knowledge and understanding of catastrophic cyber risks build. The recent cyber ILS transactions demonstrate there is appetite among capital market investors for cyber risk. However, attracting a significant uplift in risk-absorbing capacity will likely require a range of initiatives. Rather than simply mimic what has worked well for Nat Cat, including targeting the same investors and deploying similar instruments, further innovation will be necessary to make cyber risks more attractive to third-party investors, these include:

- Moves towards policy standardisation. This need not mean uniform policies per se. Instead, policy wordings that are simpler, clearer and avoid (as far as practicable) insurance-specific legalese would encourage more capital to back extreme cyber risks that firms and households may be ill-placed to absorb.
- Improvements in formal modelling and quantification of cyber risks. As understanding of cyber risks expands and as more empirical data about the anatomy of cyber incidents (especially major loss events) are captured and analysed, models will advance. This will help push out the boundaries of insurability and foster appetite for cyber risk among re/insurers and third-party investors.
- Granular re/insurance coverages that better match investor risk preferences. Insurance contracts could also be designed explicitly to differentiate coverage for different cyber-related perils or for attritional versus catastrophic cyber losses. More targeted excess-of-loss reinsurance covers that respond to specifically defined catastrophic cyber scenarios could also make it easier to tap traditional as well as alternative capital to reinsure such peak risks.

Together these innovations will boost confidence in the possible scale of transferred cyber losses and how they might covary with the returns on other financial assets. Similarly, although not peculiar to cyber, initiatives that increase the overall tradability of ILS and thereby boost

4 The amount of cyber insurance limit outstanding for the whole industry is hard to assess, but some commentators suggest it could be in the range of USD 400–450 billion, based on private conversations with market participants. See Johansmeyer 2023.

5 One interviewee opined that perhaps 5–10% of existing ILS fund capacity could, in principle, be allocated to cyber, in the sense that asset managers already have mandates to underwrite cyber risks. This might indicate a possible near-term achievable market of USD 5–10 billion, although that would happen slowly, with perhaps a more achievable issuance of USD 2–3 billion within the next three years.

secondary market liquidity, such as new investment vehicles and digital infrastructure, could also widen the investor base for cyber ILS.

Moreover, capital market involvement in assuming peak cyber risks should not be seen solely through the lens of ILS, many of which developed for natural catastrophe perils that do not share the same risk profile as cyber. Broader risk transfer solutions can, and do, also play a role, including vehicles that use traditional re/insurance balance sheets to transform cyber risks into investable propositions. Different financing vehicles and instrument structures will appeal to a wider pool of investors with diverse risk appetites, especially those who are more comfortable with ambiguity over the size and likelihood of cyber exposures and/or assuming systematic (i.e. non-diversifiable) risks.

Intrinsic uncertainties about future catastrophic cyber losses ultimately limit the extent of cyber risk transfer, whether that be to re/insurers or financial market investors. But by spreading peak risks across multiple balance sheets, ongoing financial innovation can nonetheless better align capital against cyber exposures and thereby help progress towards more optimal risk sharing.

References

Allianz. 2024. *Allianz Global Insurance Report 2024*: *Transformative years ahead for the insurance sector.* https://www.allianz.com/en/economic_research/insights/publications/specials_fmo/2024_05_23-Global-Insurance-Report.html

American Academy of Actuaries. 2021. *Cyber Risk Reinsurance Issues. Cyber risk toolkit.* https://www.actuary.org/sites/default/files/2023-02/6Reinsurance.pdf

CyberCube. 2024. *Projecting Cyber Insurance Growth: A 10-year US market outlook.* https://insights.cybcube.com/projecting-cyber-insurance-growth-report

Gallagher Re. 2024. *1st View. Balance maintained.* https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/news-and-insights/2024/july/gallagerre-1st-view-balance-maintained.pdf

Howden. 2024. Cyber Insurance: Risk, resilience and relevance. https://www.howdengroupholdings.com/sites/default/files/2024-06/howden-2024-cyber-report.pdf

Johansmeyer, T. 2023. How Big Is the Cyber Insurance Market? Can It Keep Growing? *Lawfare.* https://www.lawfaremedia.org/article/how-big-is-the-cyber-insurance-market-can-it-keep-growing

Risk & Insurance. 2024. U.S. Cyber Insurance Market Slows, Adapts in 2023. https://riskandinsurance.com/u-s-cyber-insurance-market-slows-adapts-in-2023/