THE GENEVA ASSOCIATION

INSURANCE FOR A BETTER WORLD

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

December 2024

THE GENEVA ASSOCIATION

INSURANCE FOR A BETTER WORLD

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

Darren Pain
Director Cyber | Evolving Liability,
Geneva Association

Geneva Association

Geneva Association was created in 1973 and is the only global association of insurance companies; our members are insurance and reinsurance Chief Executive Officers (CEOs). Based on rigorous research conducted in collaboration with our members, academic institutions and multilateral organisations, our mission is to identify and investigate key trends that are likely to shape or impact the insurance industry in the future, highlighting what is at stake for the industry; develop recommendations for the industry and for policymakers; provide a platform to our members and other stakeholders to discuss these trends and recommendations; and reach out to global opinion leaders and influential organisations to highlight the positive contributions of insurance to better understanding risks and to building resilient and prosperous economies and societies, and thus a more sustainable world.

Photo credits:
Cover page – Getty images on Unsplash

Geneva Association publications:
Pamela Corn, Director Communications
Hannah Dean, Editor and Content Manager
Jooin Shin, Digital Content & Design Manager

Suggested citation: Geneva Association. 2024.
Catalysing Cyber Risk Transfer to Capital Markets: Catastrophe bonds and beyond.
Author: Darren Pain. December.

© Geneva Association, 2024 All rights reserved
www.genevaassociation.org

Contents

ACKNOWLEDGEMENTS

This report has benefitted significantly from input from the members and affiliates of the Geneva Association's Cyber Working Group as well as various external interlocutors who kindly agreed to share their expert insights as background to the study. Special thanks go to:

- Richard Pennay (Aon Securities)
- Daniel Carr (Ariel Re)
- François Divet (AXA Investment Managers)
- Kyle Freeman (AXIS)
- Henry Skeoch and Richard Gray (Beazley)
- Taijaun Talbot (Bermuda Monetary Authority)
- Matt Provost (Chubb)
- David Ross (Envelop)
- Joanna Syroka (Fermat Capital Management)
- Theo Norris (formerly of Gallagher Re)
- Jess Fung, Shu Iida and Zain Hussain (Guy Carpenter)
- Tom Beckmerhagen (Hannover Re)
- Matthew Swann (Integral ILS)
- Mike Millette (Hudson Structured Capital Management)
- Luca Albertini (Leadenhall Capital Partners)
- Albert Selius (One William Street Capital Management)
- Philippe Trahan (formerly of Ontario Teachers' Pension Plan)
- Tom Johansmeyer (Price Forbes Re/University of Kent)
- Vincent Bernas, Andy Palmer, Len Zaccagnino (Swiss Re)
- Manjit Varwandkar (RenaissanceRe)
- Raffaele Dell'Amore (SIGLO Capital Advisors)
- Simon Parten (Schroders Capital)

as well as one additional interviewee who wished to remain anonymous.

Foreword

In a world where technological advancements are redefining how we live and work, cybersecurity risks have emerged as some of the most pressing challenges of our time. These risks are global, ever evolving, and increasingly complex, threatening businesses of all sizes in ways that were unimaginable just a decade ago.

To address these vulnerabilities, the insurance industry has stepped in with cyber insurance, a pivotal tool in mitigating these modern challenges. The cyber-insurance market has enjoyed impressive growth over the past decade, with global cyber premiums increasing from less than USD 1.5 billion in 2013 to around USD 15 billion in 2023. However, this still only comprises less than 1% of the total P&C insurance market.

As cyber threats grow in scope and sophistication, the cyber-insurance market faces a critical task: aligning risk-absorbing capacity with the ever-increasing need for protection. Persistent hurdles, such as attracting sufficient capital and managing systemic uncertainties, continue to limit growth. Alternative risk transfer (ART) solutions, such as insurance-linked securities (ILS) – financial instruments that bundle insurance risks into investable assets – offer potential avenues for bridging this protection gap.

This report explores the opportunities and challenges of scaling ILS for cyber, highlighting the intersections of insurance innovation and capital-market engagement. Drawing on insights from industry leaders and real-world case studies, it finds that attracting a significant uplift in risk-absorbing capacity through ILS will require a range of initiatives, including policy standardisation, improved risk modelling, and enhanced ILS market liquidity.

We hope this report fosters a deeper understanding, particularly among insurers and investors, of the dynamics shaping the evolving landscape of cyber-risk transfer, driving progress on efforts to safeguard our increasingly interconnected world.

Jad Ariss
Managing Director

Executive summary

Transforming cyber risks into investable propositions for financial markets will help attract the additional capital needed to upsize the cyber insurance market and boost societal resilience.

The digital age has fostered new opportunities for innovation and growth but also created new sources of cybersecurity risk, whether from malicious or accidental disruptions. According to the 2024 Allianz Risk Barometer, cyber incidents such as ransomware attacks, data breaches and IT outages have become the biggest worry for companies globally, with more than a third of survey respondents ranking cyber as their most important risk.

Against that background, cyber insurance has developed rapidly. Global cyber premiums 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. 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.

Cyber insurance has evolved rapidly in recent years but the protection gap for cyber risks remains huge.

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.

However, realising such continued strong growth in cyber insurance will depend crucially on attracting additional capital to absorb potential unexpected losses, especially since primary insurers cede around 50% of their cyber premiums to reinsurers, far more than other insurance lines. Alongside broadening traditional re/insurance participation in underwriting cyber risks, tapping additional risk-bearing capital from outside the sector (especially from financial markets) will likely also be essential. The size of possible extreme cyber losses is too large and/or uncertain for traditional re/insurers to carry alone.

Extreme cyber losses might be too large and/or uncertain for re/insurers to carry alone and additonal risk-bearing capacity from capital markets will likely be needed.

Since at least the late 1980s re/insurers have developed various structures to allow third-party investors to access insurance risks. These so-called alternative risk transfer (ART) solutions typically involve either dedicated risk-bearing entities – for example, separate corporate vehicles that ringfence a particular book of insurance policies – or financial instruments such as insurance-linked securities (ILS) that bundle together specific risks into a distinct investable asset – for example, catastrophe (Cat) bonds that reimburse insurance claims if major losses from a pre-defined event, such as a hurricane, occur.

ART, and in particular ILS, have so far mostly focused on property insurance, especially losses arising from natural disasters. Recently, however, a few ILS have referenced cyber risks – for example, since the start of 2023 at least five different re/insurers have issued cyber ILS, including the first fully securitised cyber catastrophe bonds. This marks an important milestone for the cyber insurance market, although the USD 800 million worth of cyber Cat bonds issued still represents less than 1.7% of the total catastrophe bond market. A key issue therefore 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 risks to those most willing and able to absorb them.

Market intelligence gathered from discussions with ILS experts suggests a cyber ILS market in development rather than on the verge of lift-off. Despite the pivot in favour of tradable securities, especially cyber catastrophe bonds, the cost of risk transfer remains high. The issuance spreads on the initial cyber bonds indicate the risk compensation required by third-party investors is larger than for natural catastrophe perils. 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 more regular cyber ILS.

A nascent ILS market for cyber has emerged, especially since 2023, though the cost of risk transfer remains high.

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.

Some of these headwinds will no doubt subside as overall knowledge and understanding of catastrophic cyber risks build. But continued innovation by re/insurers can help foster future cyber ILS, including:

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

Larger and more regular transfer of peak cyber insurance risks to broader financial markets hinges on lower costs of third-party capital and continued re/insurance product innovation.

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 ART 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.

1 Introduction

Introduction

Expanding risk-absorbing capacity for cyber is vital given the size of the protection gap and the ever more hostile threat landscape.

Over the past decade or so, the world has witnessed a dramatic increase in cyber threats. The digital age has fostered new opportunities for innovation and growth but also created new avenues for cyber adversaries (from hacktivists and cybercriminals to state-sponsored attackers) to exploit and cause damage. Equally, the proliferation of the internet and enhanced interconnectivity across organisations has heightened vulnerabilities to accidental (i.e. non-malicious) incidents that can cause serious and widespread economic disruption.

Ongoing and deepening digitalisation has driven up cyber risk exposures significantly in recent years.

According to the 2024 Allianz Risk Barometer, cyber incidents such as ransomware attacks, data breaches and IT outages have become the biggest worry for companies worldwide. More than a third of survey respondents globally (36%) rank cyber as the most important business risk, for the third year in a row.[1] The ongoing development and diffusion of new digital technologies, such as artificial intelligence, is only likely to deepen societies' exposure to cyber risks and reinforce that trend.

Against that background, 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.[2] 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.

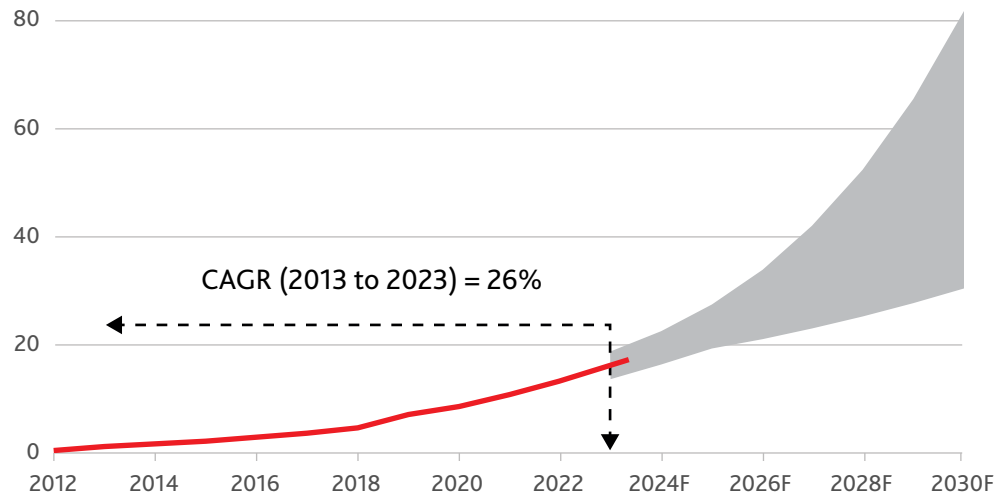
As societies continue to digitalise, ever larger cyber risk exposures will provide significant headroom for cyber insurance to grow further and help narrow what is a large and persistent protection gap.[3] Industry predictions are for the cyber insurance market to expand significantly over the next few years, although premium projections differ widely (Figure 1). Some market participants even speculate that, based on its current trajectory, cyber insurance could become bigger than some traditional P&C lines by 2040.[4]

Standalone cyber insurance has developed and matured rapidly, but the vast majority of cyber risks remain uninsured.

1 Allianz 2024a.
2 Howden 2024a; Allianz 2024b.
3 Some commentators estimate an overall implied cyber protection gap of USD 0.9 trillion or more than 99% of total economic losses. See for example, Global Federation of Insurance Associations (GFIA) 2023.
4 Gallagher Re 2022.

FIGURE 1: CYBER INSURANCE MARKET OUTLOOK – GLOBAL PREMIUM PROJECTIONS

USD billion



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

The cyber insurance market is expected to continue to grow robustly as firms and consumers become more aware of cyber risk and their lack of protection against it.

Part of the reason for the dispersion in cyber premium forecasts reflects uncertainty over the future path for the cost of insurance protection, which may not be captured well by simply extrapolating the exponential growth in nominal premiums observed over the past decade. After an extended period of stability, premium rates almost tripled in 2021 and 2022, before falling more recently. Even if pricing does not provide the uplift to premiums it did in some earlier years, most industry commentators nonetheless expect continued and substantial upward momentum in the market. That reflects an anticipated increased take-up of cyber insurance across sectors and countries, as firms' and individuals' awareness of cyber exposures rises and recognition of their degree of underinsurance grows.

1.1 Reinsurance/retrocession capacity constraints

Realising such continued rapid growth in cyber insurance will, however, 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.[5]

Insurers rely heavily on reinsurance to manage their cyber exposures but reinsurers' risk-absorbing capacity is ultimately limited.

To some extent, global reinsurers may be able to diversify their cyber exposures, especially if there are geographical differences in the risks ceded from domestically focused insurers. Such diversification, however, reduces but does not eliminate risk. Reinsurers must therefore look to hedge part of the assumed risk through retrocession (i.e. purchasing reinsurance from another reinsurer or a third

5 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.

party) or hold sufficient financial capital to ensure they can absorb large, unexpected losses up to an acceptable confidence level. Given the concentrated nature of the cyber reinsurance market – 10 reinsurers reportedly make up over 80% of capacity – retrocession capacity is limited.[6] Not only do incumbent reinsurers want to avoid any potential increase in accumulation and concentration risks across their cyber portfolio, but they may be loath to share underwriting and claims data with retrocessionaires that would otherwise be their competitors.[7]

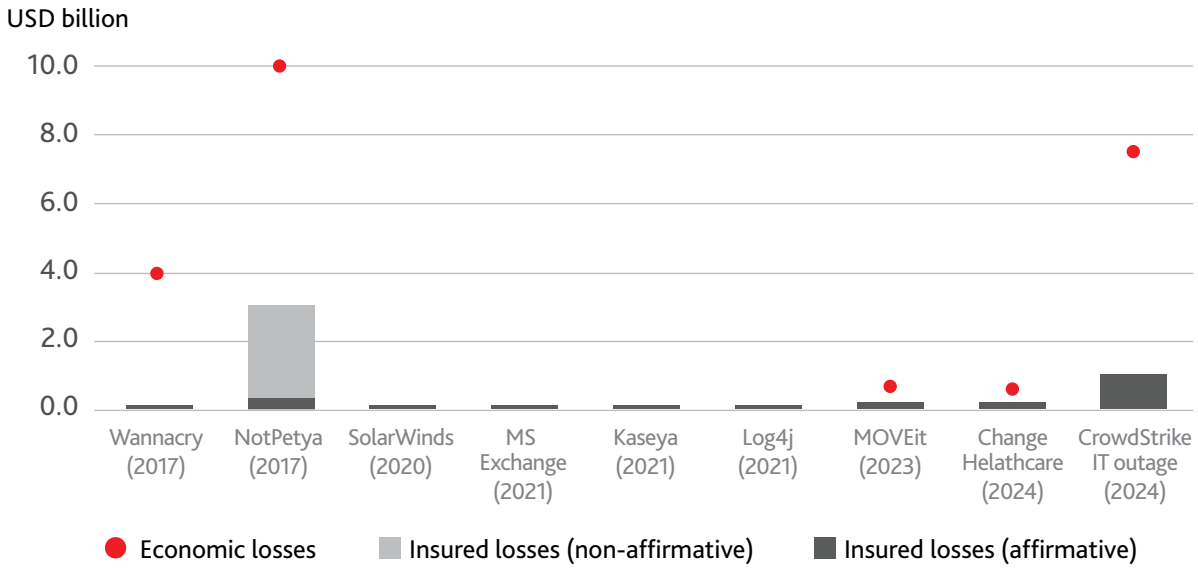
Additional third-party capital will therefore be needed to absorb potential extreme cyber losses if the cyber insurance market is to fulfil its potential.

Constraints on traditional reinsurance/retrocession do not currently appear to be binding. However, recent episodes have sharpened attention on the scale of losses that could arise from a cyber incident, including an accidental single point of failure (e.g. CrowdStrike outage in July 2024) or an indiscriminate ransomware attack that spreads across sectors and triggers financial losses for multiple insureds simultaneously (e.g. MOVEit in May 2023). With the threat environment becoming increasingly hostile, not least because of heightened geopolitical uncertainty, fears persist that a major cyber catastrophe could yet hit, generating significant accumulated losses for re/insurers.

So far, the cyber losses from high-profile incidents have remained manageable. Individually too, they have not all met the threshold that many ascribe to a catastrophic cyber event, certainly compared with the economic losses and associated insurance claims following a major natural disaster (see Figure 2).[8] But the events highlight the challenges in understanding and predicting the frequency and severity of losses given the many factors that can affect the duration of IT outages, spillover effects and liability exposure.

Furthermore, the recent bunching of cyber incidents also raises the prospect that reinsurance might be unexpectedly triggered if a collection of cyber incidents were to happen within a single treaty period. According to Guy Carpenter, had losses from the spate of recent high-profile cyber incidents aggregated within an annual reinsurance agreement, they would amount to a typical major Cat event.[9] Such smaller, accumulating events are even more difficult to predict and, therefore, hard to model accurately, which could further reduce reinsurer appetite for peak cyber risks.

FIGURE 2: ESTIMATED INSURED AND ECONOMIC LOSSES FOR RECENT HIGH-PROFILE CYBER INCIDENTS



*Loss development based on a range of early market estimates

Source: Data from Howden, PCS, Parametrix, T. Johansmeyer and CyberCube

6 Howden 2024b.
7 Artemis 2023a.
8 Verisk's Property Claim Services (PCS), a provider of insurance loss estimates, designates an event to be a cyber catastrophe when the overall insured loss exceeds USD 250 million. See Verisk 2024.
9 Guy Carpenter 2024a.

1.2 Alternative risk 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.[10] 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.

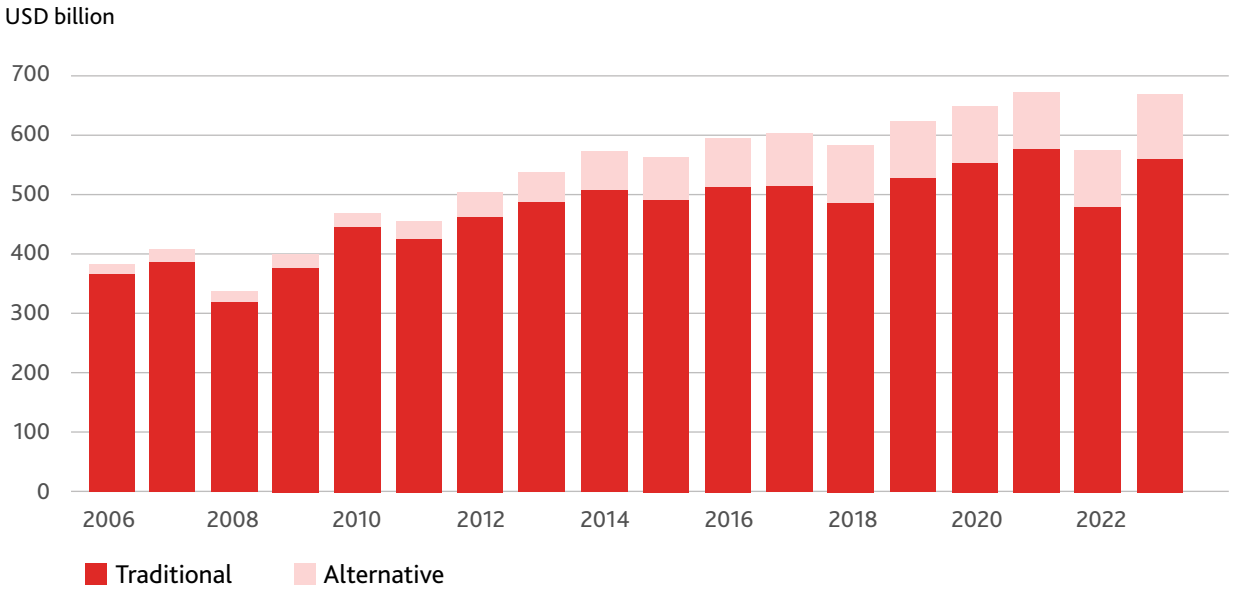
Packaging cyber risks into investable propositions for financial markets is a promising way to source additional capital for peak cyber risks.

Globally, assets under management (AuM) in alternative investments – non-traditional assets and investment strategies such as hedge funds and private equity – which are probably the most readily attractable source of funds to back cyber risks, were around USD 16.3 trillion at the end of 2023. This compares with capital in the non-life re/insurance sector of USD 2–2.5 trillion, of which reinsurers account for a little under USD 600 billion.[11]

The re/insurance industry has a long pedigree of sourcing alternative capital to augment funds raised from its own debt and equity holders. Since at least the late 1980s re/insurers have developed various structures to finance or transfer insurance risks to capital markets or specialised investors.[12] These so-called alternative risk transfer (ART) solutions typically involve either dedicated risk-bearing entities – for example, protected cell companies (PCCs) or similar corporate vehicles that ringfence the asset and liabilities of a particular book of insurance policies – or financial instruments such as insurance-linked securities (ILS) that bundle together specific risks into a distinct investable asset.[13]

In general, ART mechanisms allow investors to participate directly in selected insurance risks, often for a specified period, without necessarily buying an equity stake in re/insurance companies. According to Aon, at close to USD 110 billion at the end of 2023, alternative capital collectively accounts for around 16% of all reinsurance capital, up from 4% in 2006 (Figure 3).

FIGURE 3: GLOBAL REINSURER CAPITAL



Source: Data from Aon Securities

10 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 2024a.

11 The alternative investments figure is from Preqin's Future of Alternatives 2028 report as reported in Linna 2023. The insurance sector capital is based on Swiss Re estimates (reported in Artemis 2019a) and the figure for reinsurance capital – traditional debt and equity – is from Aon (as reported in Reinsurance News 2024).

12 The first ART transactions developed during the 1970s and involved alternative carriers like captives and captive-like structures. The first ART products used by insurance companies were life insurance securitisations developed during the late-1980s. Njegomir and Maksimović 2009.

13 As well as ILS, other financial instruments such as derivatives and contingent debt/equity can also be deployed as part of ART strategies.

ART, and in particular ILS, have so far mostly focused on property lines, especially natural catastrophe (Nat Cat) insurance. Recently, however, a few ILS have referenced cyber risks – for example, since the start of 2023 at least five different re/insurers have issued cyber ILS, including 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). Although the amount of transferred cyber risk via these bonds (at 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.[14]

Traditionally, ILS have been used for property risks like Nat Cat, but recently a nascent cyber ILS market has emerged.

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. Drawing on both desk-based analysis and market intelligence gathered from interviews with ILS experts, this report seeks to evaluate qualitatively the prevailing appetite of re/insurers and investors to exchange peak cyber risks and the factors that could shape and catalyse future cyber ILS and other ART solutions.

1.3 Structure of the report

The report is comprised of four subsequent sections. Section 2 provides background information about ILS markets and how they operate. This is followed in section 3 by a synthesis of ILS experts' views about the recent cyber Cat bonds and the persistent challenges highlighted by the deals. In light of those findings, section 4 discusses some potential initiatives that could support and ultimately promote increased transfer of peak cyber risks to capital markets. Finally, section 5 offers some concluding remarks.

14 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.

2 Existing ILS markets: Instruments, participants and practices

Existing ILS markets: Instruments, participants and practices

ILS primarily cover natural catastrophe risks, but a nascent market for cyber ILS has started to emerge in recent years.

The roots of the ILS market can be traced back to the early 1990s.[15] In the wake of significant insured losses from Nat Cat events in the U.S. – especially Hurricane Andrew in 1992 and the 1994 Northridge California earthquake – traditional re/insurance capacity became severely constrained. This prompted increased focus on capital management across both the life and non-life re/insurance sectors, and the search for ART solutions to source additional risk-bearing capital. Arguably, ILS offered the most straightforward access to capital markets because they could be structured based on instruments with which financial market investors were already familiar.

2.1 Types of ILS

ILS is a broad category used to refer to a range of risk transfer instruments. In general, there are four main types: two tradable instruments (catastrophe bonds and industry loss warranties (ILWs)), and two which involve privately arranged contracts between investors and a risk carrier (collateralised reinsurance and sidecars). Private contracts are often more complex and less standardised, making it harder to establish a secondary market for them.

There are four main types of ILS: Cat bonds, industry loss warranties, collateralised reinsurance and sidecars.

In addition to being tradable, a key feature of Cat bonds and ILWs is the non-proportional nature of the cover (i.e. losses above a certain threshold – the attachment point – are transferred to investors up to an agreed limit – the exhaustion point). Compared with traditional reinsurance, the attachment point for such excess-of-loss structures is typically higher. Collateralised reinsurance may also offer excess-of-loss protection, although this is typically on an aggregate basis (i.e. for cumulative losses over multiple events throughout the contract period). Sidecars by contrast are usually proportional (e.g. quota share) covers, with investors taking on a pre-determined share of all losses (and profits) on specific business, up to the limit of the contract.

The main risks referenced in ILS relate to insured property losses from natural catastrophes such as hurricanes or earthquakes. Private transactions, however, give investors access to a wider range of insurance perils than those available in the Cat bond market – including marine, aviation and other specialty risks – and a broader range of investment structures. They are also typically shorter in length (usually a one-year term compared with around three years for a Cat bond) – see Table 1.

Each type of ILS has its distinguishing features (see Box 1) although some of these can be replicated or removed to create instruments with different risk/return profiles. For example, ILWs may be securitised into Cat bonds or they can be organised as private, customisable reinsurance contracts without a full securitisation process. Similarly, collateralised reinsurance can be structured as a tradable security – so-called Cat-bond-'lite' transactions – with scope for secondary transferability.

15 The first ILS contracts covering property catastrophe risks originated in the London Market in the late 1980s. It was not until the mid-1990s, however, when AIG, St Paul Re, Hannover Re and USAA developed innovative bond-type structures giving investors direct access to the returns from natural catastrophe insurance, that the market expanded significantly. See DiFiore 2019.

TABLE 1: MAIN ILS INSTRUMENTS

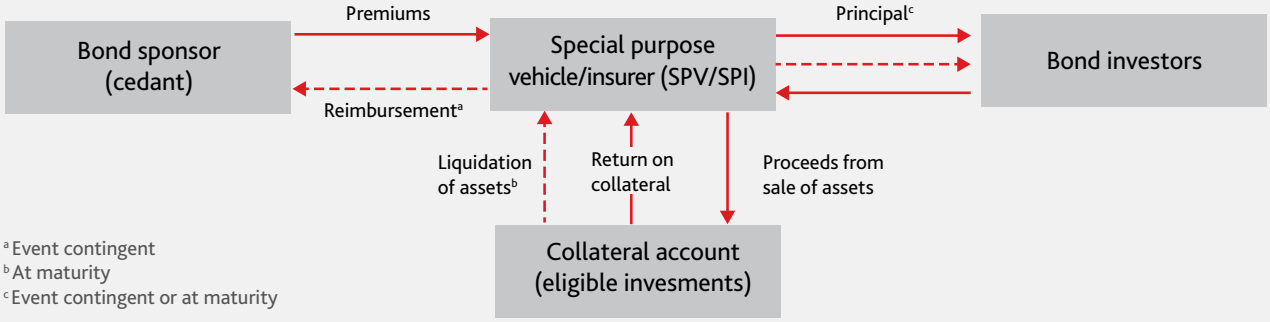
	Tradable instruments		Private contracts	
	Catastrophe bond	**Industry loss warranty**	**Collateralised reinsurance**	**Reinsurance sidecar**
Description	Debt security that pays the issuer when a pre-defined disaster, such as a hurricane, occurs.	Reinsurance or derivative-based instrument that compensates the holder based on total industry losses from a specific region/peril combination.	Bespoke reinsurance contract where collateral equal to the exposure limit is held in trust either until maturity or on the occurrence of a pre-defined event.	Separate legal entity created by re/insurers, that allows third-party investors to share proportionally in the profits/losses on a group of re/insurance policies.
Typical perils covered	Natural catastrophe Extreme mortality Cyber Terrorism Mortgage	Natural catastrophe Marine Energy	All perils	All perils
Typical maturity	2 to 5 years	1 year	1 to 3 years	1 year
Trigger type	Indemnity Index Parametric	Industry index	Indemnity	Indemnity
Basis of coverage	Excess-of-loss (per event or aggregate)	Excess-of-loss (per event or aggregate)	Proportional (quota share) or excess-of-loss (aggregate)	Proportional (quota share)

Source: Geneva Association, based on published sources

Box 1: ILS structures

Catastrophe bonds. A high-yield debt instrument that provides the issuer (i.e. cedant) with protection against catastrophic losses if specific conditions, such as an earthquake or hurricane, occur. The usual structure involves a special purpose vehicle (SPV) or insurer (SPI) entering into a reinsurance agreement with the bond sponsor, receiving premiums in exchange for providing the coverage.[16] The SPV issues the securities to investors, the funds from which are deposited into a collateral account and typically invested in highly rated money market instruments. Should a qualifying catastrophe happen, the investors lose all or part of the principal and the sponsor receives that money to cover their losses. If no qualifying event occurs during the life of the bond the principal is returned to investors along with any accrued interest. The structure of cash flows is summarised in Figure 4.

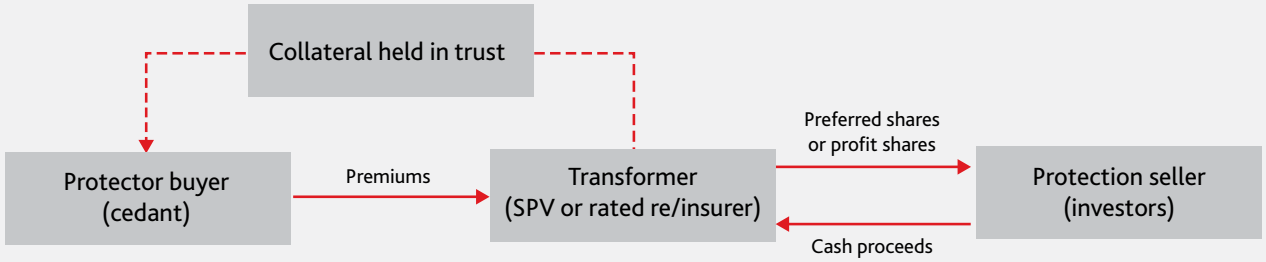
FIGURE 4: TYPICAL CAT BOND STRUCTURE



Source: Geneva Association, based on published sources

Collateralised reinsurance (ColRe). Technically, ColRe is little different from traditional reinsurance except that an SPV often stands between the cedant and investors and collateral is provided upfront (see Figure 5).[17] The collateral – a combination of premiums paid by the cedant and capital provided by the investor – is typically held in a trust account to cover potential claims.[18] If a loss event arises, part or all of the collateral will be used to reimburse insured losses. If no losses occur, the collateral assets plus any associated investment income are returned to the investor.

FIGURE 5: STRUCTURE OF A COLLATERALISED RE/INSURANCE TRANSACTION



Source: ILS Bermuda[19]

16 The SPV is necessary otherwise investors would be directly offering insurance to the issuer, which is not permitted without regulatory authority. The SPV is therefore also sometimes called a 'transformer' because as a licenced insurer, it transforms the investment of funds by the investors into a sale of insurance.

17 An SPV may not be needed if investors work with a fronting re/insurer to access insurance risks. In that case, the fronting carrier may require less than full collateral, albeit it will usually charge a fee for retaining any residual exposure.

18 The assets in the trust account are segregated from other assets in case of insolvency and contractual provisions determine the release of the collateral. See ILS Bermuda.

19 Ibid.

Industry loss warranties (ILWs). These are reinsurance or derivative contracts that pay out if the insurance industry's aggregate loss from a covered event exceeds a particular threshold, usually measured according to an index. The protection seller receives a premium for providing cover up to a specified limit which is the amount of compensation the protection buyer receives if the ILW is triggered. Additional conditions sometimes must be met for a payout to be made. For example, in addition to the overall industry loss, the buyer must also have experienced a specified amount of loss themselves.[20] Similar to a Cat bond, collateral is held for the length of the ILW's term and is released at the end if there is no qualifying loss. Unlike Cat bonds/ColRe, ILWs often feature reinstatement provisions that automatically reset coverage following a triggering event (upon payment of an additional premium).

Reinsurance sidecars. These are limited purpose reinsurance companies that assume a portion of the ceding company's underwriting risk (including losses and expenses) over a defined period and for certain insurance policies, in exchange for a premium. Sidecars usually rely on quota-share reinsurance instead of excess-of-loss reinsurance that is characteristic of Cat bonds and ILWs.

Source: Geneva Association, based on published sources

ILS are typically issued via private placement to a selected group of investors rather than offered to the general public. But the contractual format can have important implications for the subsequent tradability of the security. U.S. government regulations restrict how securities can be marketed to prospective investors both at initial issuance and subsequent resale, including the amount of background information disclosed (see Box 2). In practice, so-called Rule 144A bonds have emerged as a preferred format for Cat bonds since they streamline the placement process for a sophisticated investor base that typically invests in ILS.

Box 2: SEC registration restrictions

According to the U.S. Securities Act of 1933, issuers of securities, such as bonds, must register them with the Securities Exchange Commission (SEC) and provide extensive documentation before they can be offered to the general public. In particular, standard information covenants prescribe required disclosure to investors both at the date of issuance and on an ongoing basis. However, if the securities are privately placed – i.e. sold to a select group of investors and institutions rather than via a public offering – a variety of registration exemptions apply.

Rule 144A

Under Rule 144A, qualified institutional buyers (QIBs) – broadly, institutional investors that own or manage on a discretionary basis at least USD 100 million worth of assets – are permitted to trade securities freely amongst themselves within the U.S., bypassing the normal SEC registration and allowing for bespoke information disclosure. A sister regulation – so-called 'Regulation S' – allows for offers and trades of bonds outside the U.S., serving both U.S. and non-U.S. QIBs.[21] The rationale for the rule is that these sophisticated investors do not require as much information and protection as individual investors.[22]

Section 4(a)(2)

Section 4(a)(2) also exempts from registration offers and sales by the issuer that do not involve a public offering. The exemption only applies for that initial private placement and does not exempt the securities from potential registration in the future, including in the event of resale. In short, Section 4(a)(2) lets companies sell securities in a private sale without registering them, but buyers of those securities cannot usually resell without registering them.

Section 4(a)(1)

Section 4(a)(1) exempts the holder of securities issued in a private placement from filing a registration statement, should they wish to sell them privately, provided they are not an underwriter (i.e. an entity that acquires securities with a view to distribution).[23] In combination with Section 4(a)(2)'s requirement that the initial sale is non-public, an individual may resell a security issued in a subsequent private placement.

Source: Geneva Association, based on published sources

20 Artemis.
21 Balalaeva 2024.
22 Technically, Rule 144A is an exemption for resales as opposed to primary issuance. Often though, securities are first privately placed with initial purchasers who then immediately resell the securities under Rule 144A to domestic and offshore QIBs. King & Spalding 2022.
23 This is sometimes referred to as Section 4(1 ½) or Section 4(a)(1 ½) private placement although it is not a formal entry in the U.S. Securities Act. See Cornell Legal Information Institute.

Whatever the ILS format, however, funds typically need to be made available upfront as collateral to ensure claims can be paid should a qualifying event occur. The proceeds from issuance are usually paid into a trust account, where they are held for the length of the contract or until a claim is paid.[24] Unlike corporate or sovereign bonds, Cat bonds and most other insurance-linked instruments are therefore not directly exposed to the default risk of the issuer. Similarly, the impact of interest rate changes on the market value of ILS investments is generally negligible since part of the coupon payment on the bond is usually based on money market returns.

For all ILS, funds are typically offered upfront to guarantee claims can be paid if a qualifying event occurs.

There are four main forms of triggers for ILS: indemnity, modelled loss, index and parametric. An indemnity trigger involves reimbursing the actual losses of the bond issuer. For example, losses arising from an earthquake in a certain area of a country. In the case of modelled loss triggers, recovery is based on expected losses derived using physical data about the catastrophe rather than actual losses incurred by the re/insurer. An industry index trigger refers to losses across the insurance sector. A parametric trigger is based on, for example, agreed criteria about the size of an earthquake such as moment magnitude – derived from an analysis of physical ground vibrations arising from the quake or shaking intensity – based on human observations and reports of shaking and damage.[25]

Usually, ILS offer single-shot protection against specified events or total annual losses, even if the contract extends over multiple years.

In contrast to traditional reinsurance, most ILS do not include reinstatement provisions that allow the insured limit to be automatically restored if it is exhausted during the coverage term. Instead, ILS normally provide single-shot protection against specified events or annual aggregate losses, even if the contract extends over multiple years. For investors, this provides comfort about the full extent of their exposure and caps the collateral they must provide. From a sponsor perspective, this feature underscores the non-fungible and non-permanent nature of ILS capital, certainly compared with debt and equity.

2.2 Role of specialist fund managers, re/insurers and intermediaries

Given the expert knowledge required to understand complex insurance risks and associated contract language, specialist asset managers have developed to attract capital from institutional investors who seek exposure to specific insurance risks via ILS. While some end-investors may choose to invest directly in ILS, the large majority tend to do so via these specialist funds, albeit the overall allocation is modest – pension and sovereign wealth funds typically allocate less than 2% of their total AuM to ILS.[26]

Most investors participate in ILS via specialist funds, often set up as mutual funds and overseen by specialist asset managers.

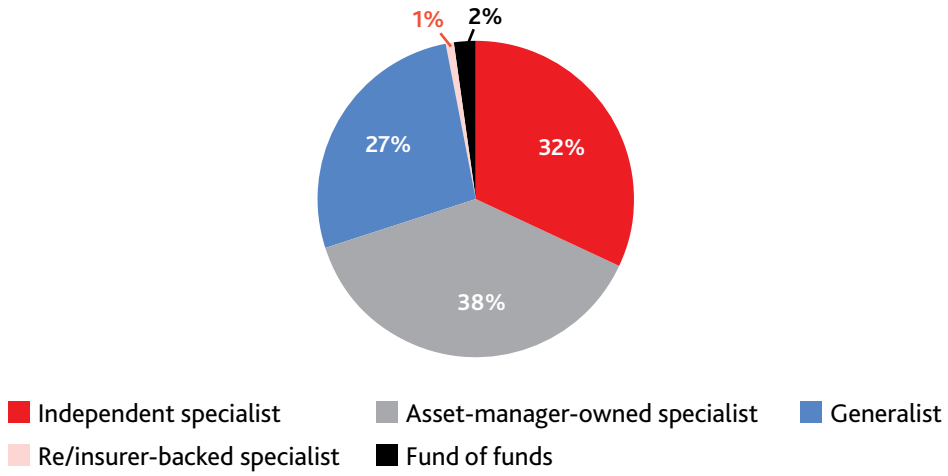
Often, ILS funds are set up as mutual funds whereby investors pool money to purchase ILS. Investors own shares of the fund, not the underlying securities, which they can typically buy and sell over the life of the fund. Alternatively, rather than a comingled fund, investors may opt for a separately managed account that directly invests in ILS on their behalf.[27] Either way, ILS asset managers aim to construct portfolios with a wide-range of risk-return profiles and strategies. Some funds will exclusively include collateralised reinsurance, Cat bonds, and other re/insurance-specific products, while others seek to blend ILS instruments with other types of financial assets.[28]

ILS funds offer their investors a variety of possibilities to withdraw their stake, anywhere from once a week (even daily for certain structures) to yearly for those who want to enter into annual reinsurance contracts alongside more liquid investments. Most funds sit somewhere between these two liquidity options.[29] For example, in Europe, Undertakings for the Collective Investment in Transferable Securities (UCITS) funds must offer redemption facilities at least twice a month.[30, 31]

24 Wright 2024.
25 U.S. Geological Survey (USGS).
26 Artemis.
27 Davis and Clark 2020.
28 Based on a sample of 21 fund managers (representing around USD 27 billion managed assets exposed to ILS across 52 different investable funds), Amici and Dell'Amore 2024 report that around a third of ILS products are overwhelmingly invested solely in public Cat bonds; another third is almost exclusively exposed to private ILS transactions; and the remainder consists of a mixed allocation to Cat bonds and private ILS.
29 Edmonds 2015.
30 UCITS are open-ended collective investment schemes established and authorised by EU law. Perceived as safe and well-regulated investments, authorised UCITS can be marketed and sold to retail investors globally.
31 European Securities and Markets Authority (ESMA) 2024a.

Some ILS fund managers may be owned or operated by re/insurers, who are often the main sponsors of ILS transactions. This sometimes helps in sourcing risks suitable to transfer to capital markets as well as deploying in-house expertise in quantifying the nature of those risks. Around a third of the ILS marketplace is organised this way (Figure 6). Most ILS funds are, however, overseen by independent or specialist asset managers or operate as business units of larger investment firms. Some of these ILS funds will set up their own licenced reinsurance companies or work with fronting carriers – licenced re/insurers who write insurance policies and cede the risk to the fund – to originate investable opportunities.

FIGURE 6: SHARE OF ILS ASSETS UNDER MANAGEMENT, BY FUND TYPE (JULY 2023)



Source: Data from Insurance Insider ILS and Artemis

Whether organised by a re/insurer or an asset manager, the nature of the initial issuance process means reinsurance intermediaries are typically actively involved in arranging and placing many ILS transactions. Broker-dealers are often influential in designing an ILS so that it appeals to prospective investors. According to data from Artemis, reinsurance broker-dealers were involved as structurers or bookrunners/managers (i.e. responsible for underwriting the issuance and marketing the securities) in more than three quarters of all Cat bond transactions (based on outstanding issuance).

Part of the job of the broker-dealer can also be explaining and interrogating the quantification of the underlying risks. Often this will draw on the expertise of third-party vendors as well as insights from in-house risk models. In the case of Nat Cat perils, there is a well-established modelling community with a long history of developing quantitative risk models. More recently, a few specialist cyber Cat modelling firms have emerged that provide risk metrics that seek to illuminate the scale and likelihood of extreme cyber insurance losses, drawing on expert-led scenario analysis.

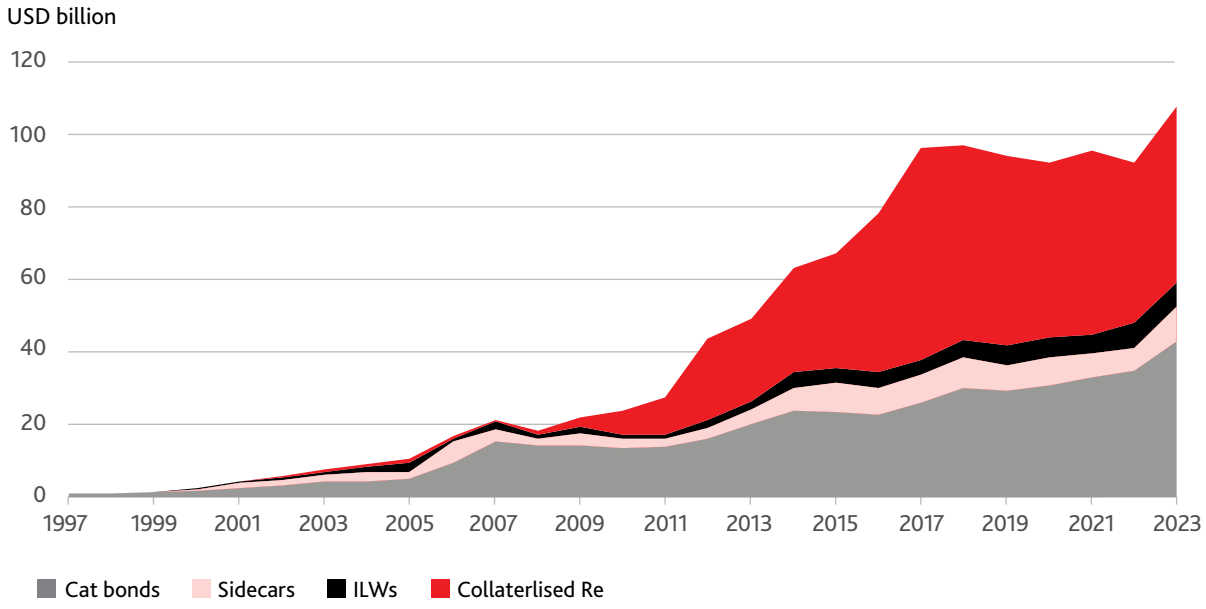
2.3 Recent ILS issuance trends

While Cat bonds are the most well-known ILS instrument, collateralised reinsurance represents the largest segment of the overall market. This reflects a rapid increase in issuance during the 2010s. More recently however, Cat bond issuance has provided the main impetus to growth in alternative capital, with collateralised reinsurance largely flatlining since 2017 (Figure 7). The Cat bond market increased by over USD 7 billion to reach USD 42 billion in outstanding issuance in 2023, up 21% from 2022.[32] In fact, at USD 15.4 billion, 2023 broke the record for the largest year of Cat bond issuance.[33]

Though collateralised reinsurance makes up the largest share of the ILS market, Cat bond issuance has seen the most growth in recent years.

32 Aon 2023.
33 BeInsure 2024.

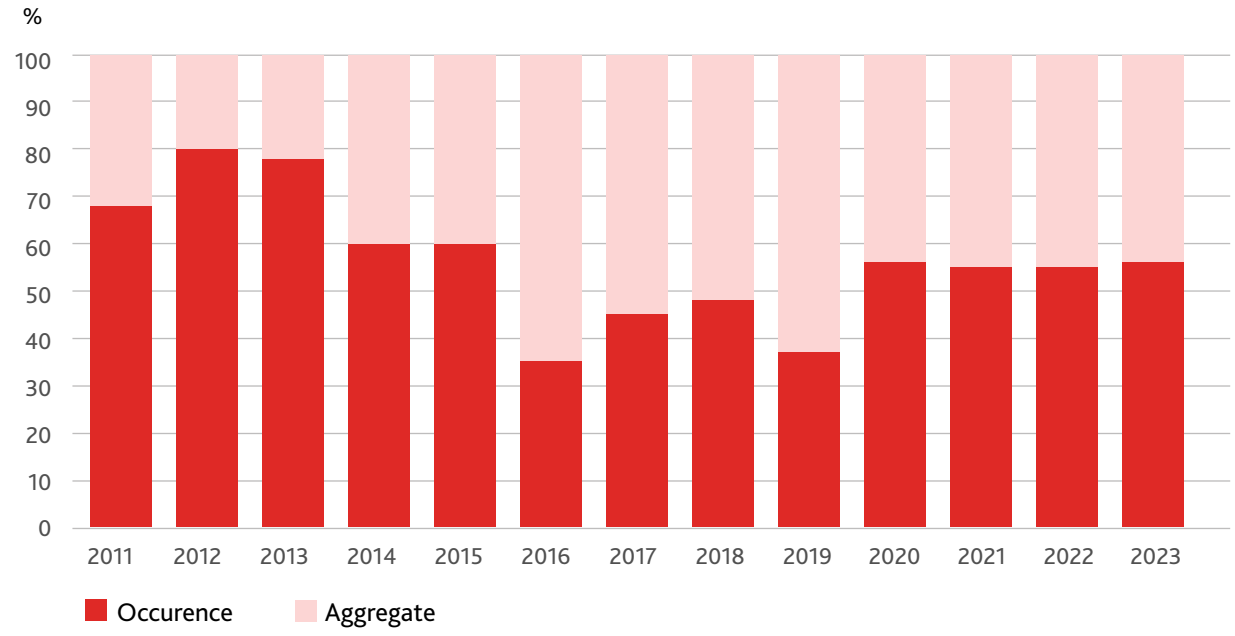
FIGURE 7: ALTERNATIVE RE/INSURANCE CAPITAL OUTSTANDING, BY ILS INSTRUMENT



Source: Based largely on data from Aon Securities

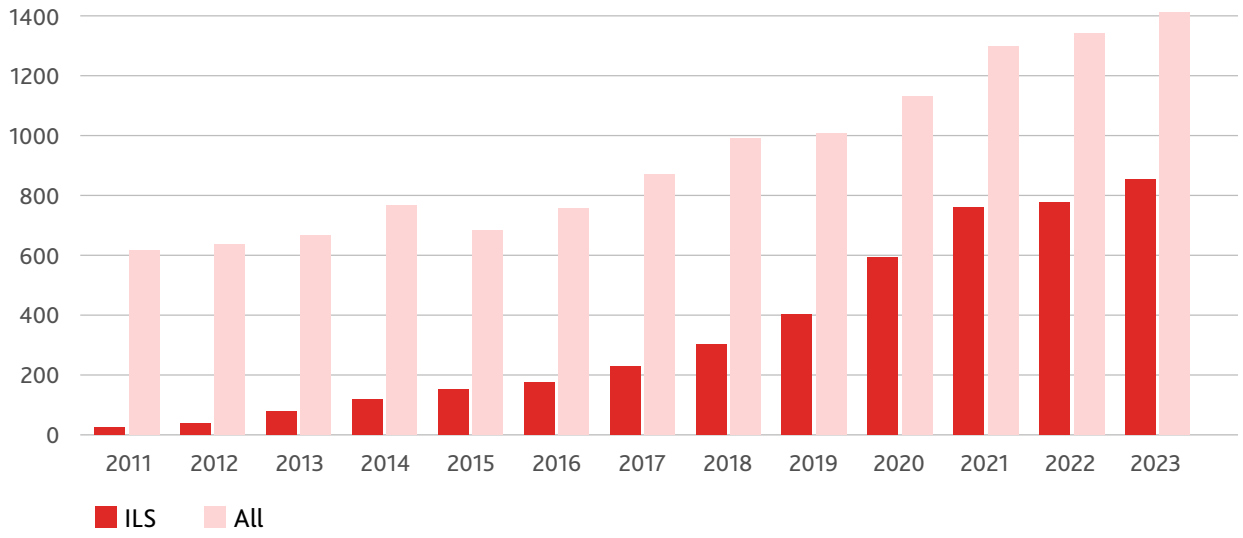
Over time, there also have been important shifts in the structure of Cat bonds. Notably, while early deals typically referenced aggregate losses for a particular peril, over recent years per occurrence transactions have become more prevalent (Figure 8). Such securities only pay out if the loss from a single event (e.g. a hurricane) exceeds a given threshold. Data from the Bermuda Stock Exchange (BSX), a favoured jurisdiction for ILS issuance, also show that the total number of listed ILS – including ILWs or collateralised reinsurance that have been transformed into tradable securities – increased from 25 in 2011 to 849 in 2023 (Figure 9). Around half the currently listed ILS refer to Nat Cat perils.

FIGURE 8: SHARE OF CAT BONDS, AGGREGATE VERSUS PER OCCURRENCE



Source: Data from Swiss Re

FIGURE 9: SECURITIES LISTED ON THE BERMUDA STOCK EXCHANGE



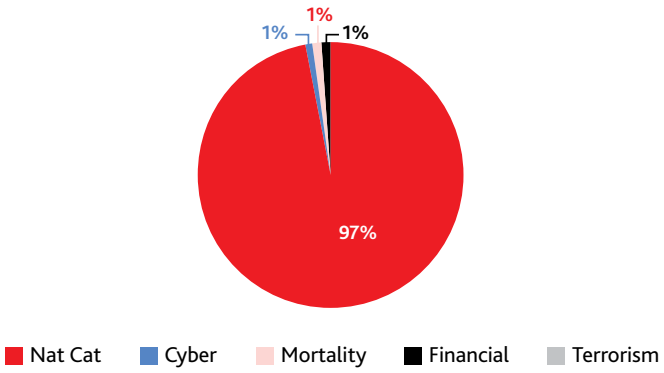
Source: Data from BSX and Artemis

The recent pick-up in Cat bond issuance occurred despite the rise in risk-free interest rates which reduced the intensity of the 'search for yield' among investors. Indeed, following a sharp general repricing of catastrophe risk across ILS and reinsurance markets, ILS investors enjoyed significant returns. According to data from the Swiss Re Cat Bond Performance Indices, overall returns on Cat bonds were 19.3% in 2023, the highest annual yield on record.[34]

2.4 A nascent cyber ILS market

The prospect of cyber ILS has been talked about for years.[35] While a few private cyber collateralised reinsurance and sidecar agreements have been transacted from around 2017, these were sporadic, involving a few selected participants.[36] For example, in 2021, Ontario Teachers' Pension Plan, a Canadian pension investment manager, reportedly participated alongside re/insurers in a financing round for the specialist cyber insurer CFC through Lloyd's newly established London Bridge Risk ILS platform.[37] Around a year later, Coalition, a technology-focused cyber insurance company, launched Ferian Re Ltd, a Bermuda-based reinsurer backed by an investor group led by BDT Capital Partners.[38]

FIGURE 10: SHARE OF CAT BONDS OUTSTANDING ISSUANCE, BY CLASS OF RISK (%)



Source: Data from Artemis

34 Swiss Re 2024.
35 For example, in 2016, Credit Suisse piloted a USD 223 million operational risk catastrophe bond that included cyber risk. See Artemis 2016.
36 See Box 5 in Geneva Association 2023.
37 Artemis 2021a.
38 Coalition 2022.

TABLE 2: 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

However, over the past two years, issuance has accelerated with several notable cyber ILS deals coming to market offering excess-of-loss coverage against specific loss events (see Table 2). This includes the first fully securitised transactions, of which six were in 144A format, albeit with relatively short maturities. Most of those bonds provided their sponsors with indemnity protection against cyber losses, although the recent deals also included the first industry-loss index and a parametric-based bond. The average exposure limit on the outstanding cyber Cat bonds is around USD 110 million, although there is a wide range of available protection across sponsors. By comparison, the 10-year average transaction size for a Nat Cat bond is U.S. 168 million.[39]

Despite the recent increased issuance, the USD 800 million worth of cyber Cat bonds outstanding still represents only 1.7% of all Cat bonds (Figure 10). Even allowing for smaller, privately structured collateralised reinsurance deals, which might collectively push the size of cyber ILS in issuance to around USD 1.5–2 billion, this remains a small share (less than 2%) of the overall ILS market.

39 Artemis 2024a.

3 Market insights from recent cyber Cat bond deals

Market insights from recent cyber Cat bond deals

The cyber ILS market is expected to expand steadily rather than drastically. Challenges like high capital and transaction costs will need to be overcome to promote the routine transfer of peak cyber risks to capital markets.

Although the overall amount of cyber risk transferred via ILS remains modest, the transactions that have been executed offer clues as to market features that may be influential in developing and sustaining future cyber ILS. This is not least because the deals themselves were the culmination of long and detailed design processes, involving considerable dialogue between sponsors and investors.

To explore this issue further, this section synthesises ILS market participants' views on recent cyber Cat bonds. It draws heavily on interviews with experts from across the re/insurance and ILS sectors – see Box 3 for more details.

Box 3: Sample of interlocutors

Since ILS are usually offered via private placement, information about all such transactions do not always reach the public domain, especially privately arranged ILWs, collateralised reinsurance and sidecars. Even when deals are reported in the press, some details remain confidential. In particular, the list of investors involved in the risk transfer is seldom revealed, unless individual institutions (e.g. a lead investor) chooses to go public about their participation.

To gain a range of perspectives on cyber ILS, interviews were conducted with different participants in the ILS market. Specifically: re/insurers who cede risks via ILS and/or invest in ILS on their own behalf or for their clients; ILS fund managers who manage monies for third-party institutional investors like pension funds and family offices; key intermediaries such as reinsurance broker-dealers; and a financial regulator from a leading jurisdiction in ILS. In total, ILS experts from around 25 organisations were interviewed, including:

- All five re/insurer sponsors of the initial cyber Cat bonds/Cat bond 'lites' issued in 2023/24.
- The two main broker-dealers involved in those cyber ILS transactions plus another major reinsurance broker and a smaller, specialist reinsurance intermediary.
- Selected ILS funds, end-investors and re/insurer asset managers who invest in cyber securities and/or other forms of cyber ART as well as some who decided not to participate in the recent cyber Cat bonds. Collectively the interviewed ILS investors manage more than USD 40 billion (or around 40% of the total ILS market).

Source: Geneva Association

3.1 Key instrument design considerations

Discussions with market participants highlighted several design features that were prominent in negotiations between ILS sponsors and third-party investors.

3.1.1 Format

The latest cyber ILS deals indicate a pivot in favour of tradable securities, especially those with a Rule 144A format. From a practical perspective, some ILS funds are constrained by their mandates to invest only in financial instruments that are tradable. For example, in Europe, UCITS funds can only invest in transferable securities and other liquid assets, making a 144A ILS almost essential for such investment schemes.[40] While private collateralised reinsurance transactions structured as bonds can in principle be traded, the format may not provide the same level of disclosure, especially beyond the primary issuance stage.[41] As a result, the resale opportunities are often more limited for private securities than a 144A.

As highlighted in Box 4, the early Cat-bond-lite deals issued over three separate tranches in 2023 helped pave the way for subsequent issuance of a full 144A cyber Cat bond. The latter was not only larger in size than the individual private transactions but also the term to maturity was longer. Anecdotal evidence also indicates the number of investors involved in the 144A bond placement increased compared with the private bond.

Box 4: Realising a vision – Reflections from a pioneering cyber Cat bond sponsor

Safeguarding policyholders against a rise in cyber risk is one of the most formidable challenges – and opportunities – facing the specialty insurance industry today. Whilst significant, thus far cyber insurance losses have thankfully been manageable, impacting re/insurers' earnings rather than their capital. However, the persistent and pervasive nature of the threat, as well as residual worries that past incidents could have been much worse had circumstances evolved differently, highlight the need for additional reinsurance capacity to protect against large and widespread accumulated claims.

Beazley identified the ILS market as a potential source of additional reinsurance capital. But historically, ILS covered peak natural catastrophe perils for the property market. Since cyber risk evolves quickly and catastrophic cyber events have a potentially very large and indiscriminate footprint, some of the traditional risk diversifiers for the property class – like industry and geography – are less relevant, although firms' different use of technology can be a diversifying factor.

Investor education was, and remains, key

There had been cyber ILS deals before, albeit these were typically private collateralised reinsurance transactions involving a small set of ILS asset managers.[42] Broader ILS market interest in cyber had been tempered by caution around an asset class that was both relatively nascent and complex. In assessing the prospects for securitising peak cyber risks, investor education quickly emerged as an essential prerequisite.

Three areas stood out:

- Dispelling common misconceptions around cyber insurance (e.g. the mistaken belief that cyber insurance pays out if there is a cyberattack upon critical national infrastructure when, in fact, most policies exclude such incidents),
- Clarifying what cyber policies cover (e.g. ensuring investors were comfortable with contract wordings, in particular event definitions, exclusions and policy limits),
- Helping investors understand the overall size of catastrophic cyber risk (e.g. using insights from third-party vendor models).

As well as confidence in the ability of the insurance sector to effectively measure extreme cyber risks, ILS investors also needed reassurance about a cedant's capability to manage that exposure. No two cyber insurers are the same, but structural organisation features may help reassure investors about the strength of a re/insurer's cyber underwriting and risk selection.

40 The EU UCITS Directive requires funds meet strict eligibility criteria such as the ability to redeem units or shares at the request of investors and to calculate the net asset value upon issuance or redemption.

41 It may be the case that more detailed information is disclosed at issuance in a private transaction compared with a 144A security, not least because it will typically be shared with only a limited number of counterparties (most notably the broker-dealer). But such information will not necessarily be publicly available to investors upon resale, which could deter prospective buyers in the secondary market.

42 Johansmeyer and Mican 2022.

For example, cyber insurance represents a significant proportion of Beazley's gross written premiums, so the class receives an extraordinarily high level of focus from Beazley's board, underwriting committee and exposure management teams.

From private ILS deals to a 144A catastrophe bond

Having cultivated investor appetite for cyber ILS, Beazley decided first to sponsor a one-year private catastrophe bond providing indemnity protection for its cyber insurance portfolio. Issued in 2023, the transaction delivered USD 81.5 million of cyber catastrophe protection across three tranches, with the second and third tranches a response to additional investor demand. A private bond was the preferred structure because it allowed for constructive input into its design from investors to facilitate broadly comparable cover to Beazley's traditional cyber reinsurance programme.

Although the structuring of the private cyber bond was years in the making, the deal subsequently enabled a much smoother and faster process around the sponsorship of a USD 140 million 144A cyber Cat bond, a format with broader appeal for ILS investors than a private bond. Effective from January 2024, the bond runs for two years through to the end of 2025.[43] Second and third 144A bonds, offering similar terms to the first, have subsequently been issued, bringing the total limit to USD 510 million and providing reinsurance out to 31 December 2027.[44]

As part of the offering for Beazley's 144A cyber Cat bond, investors had access to multiple model outputs – which is rarely seen for property Cat bonds – increasing overall comfort in modelled losses. Specifically, investors could analyse risks based upon outputs from two specialist catastrophe modelling companies, both of which had access to Beazley's detailed cyber underwriting data.[45]

Source: Contributed by Richard Gray and Henry Skeoch, Beazley

3.1.2 Structure

Many ILS investors typically want exposure to extreme cyber risks that are rare and then only for selected peak perils – exposures to routine cyber incidents offer limited benefit to their portfolios and may only create additional headaches over managing the collateral set aside if insurance claims have not fully developed by the end of the contract. It is perhaps unsurprising therefore that most of the recent cyber ILS have been structured as per occurrence, excess-of-loss ILS coverage for major incidents.[46] This echoes recent developments across the broader ILS market.

Recent cyber ILS have been structured as per occurrence, excess-of-loss coverage for major incidents, reflecting investors' desire for exposure to extreme but rare cyber risks.

That sponsors felt comfortable with occurrence-based triggers seems to reflect increased confidence among re/insurance carriers in modelling cyber scenarios, retaining more attritional losses and managing the potential for overall losses from an incident to differ from the funds recoverable via the ILS.[47] The lack of aggregate cover nonetheless leaves them vulnerable to accumulated losses from multiple events during the contract period.

3.1.3 Pricing

The pricing on the initial cyber Cat bonds suggests the compensation required by third-party investors for taking on extreme cyber exposure was larger than for other Nat Cat perils. The average multiple over modelled expected losses – a key indicator of the required risk margin – was over 8, compared with around 4 for other hard-to-model risks such as meteorite impact or volcano eruption.[48]

To some extent the outsized risk spreads on the recent cyber Cat bonds reflect a novelty or innovation premium – the extra return investors demand for investing in new financial instruments – perhaps linked to the challenges in accurately modelling future cyber losses (see Box 5). Over time, as investors become more comfortable with assuming cyber risks and as the associated ILS market matures, the novelty premium will most probably fade. In fact, since issuance, three of the four maiden cyber Cat bonds have traded above their par values, albeit in thin trading, perhaps indicating a prospective fall in required returns on future cyber risk securitisations.

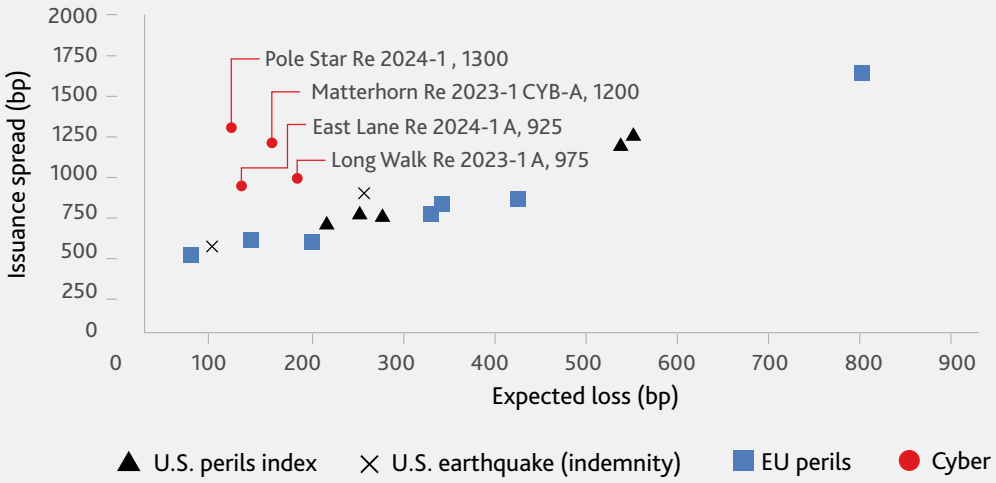
43 Beazley 2024.
44 Artemis 2024b,c.
45 RMS was the modelling agent for the 144A bond, but Beazley also paid for investors to receive a second view of risk from CyberCube, the modelling agent used for Beazley's earlier private bond.
46 Most of the 144A cyber Cat bonds in issuance have an attachment point of USD 500 million or higher.
47 Such so-called basis risk is often a core concern for ILS sponsors because it affects the accounting treatment, ratings, regulatory capital requirements and their operating result.
48 The average expected loss multiple for Nat Cat ILS is from Braun et al. 2023.

Box 5: Cyber ILS – Gauging the novelty premium

Investors often require additional risk compensation for buying a new and unfamiliar investment product, the returns on which can typically be hard to estimate. This seems to have been the case with the recent cyber ILS, not least given the complexity and specialist nature of the underlying risks. However, isolating a so-called novelty premium within the overall risk premium is not easy. In addition to fundamental factors such as the degree of uncertainty of future payouts, market frictions like illiquidity will influence the yields that investors demand.

The insurance risk spread – the component of the Cat bond yield that compensates for potential future uncertain payouts – is a function of modelled expected loss and a risk margin for unexpected losses.[49] Since projected expected loss values are just estimates of the true expected loss, uncertainty around likely future losses is itself part of the risk margin. Hence, one crude metric (at least to provide a clue of the presence if not the precise size of the novelty premium) is to assess if the risk spread on the recent cyber Cat bonds differed materially from other Cat bonds issued during the same period and/or compared with other previously newly referenced perils, after controlling for differences in their modelled expected loss.

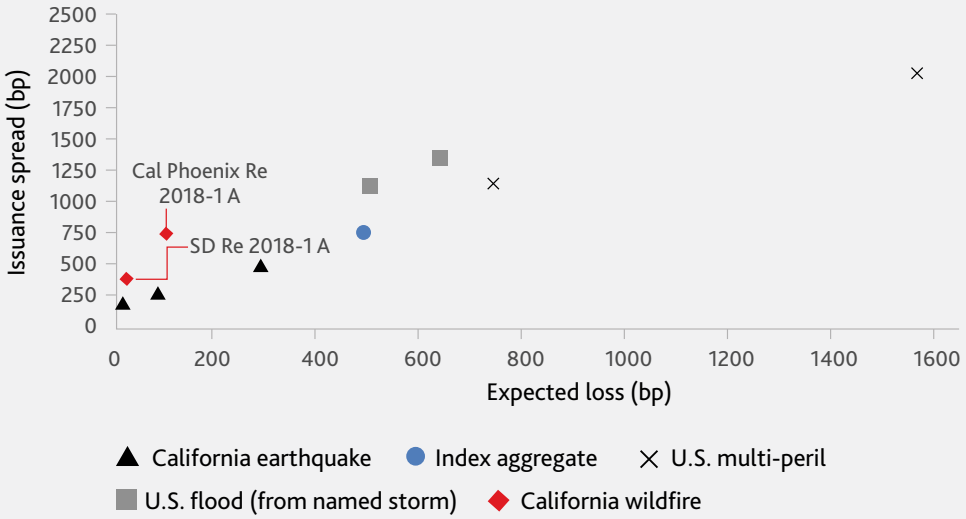
FIGURE 11: ISSUANCE SPREADS VERSUS EXPECTED LOSSES, BY PERIL (Q4 2023)



Note: Based on a subset of all bonds issued during Q4 2023, excluding, for example, some outlier U.S. windstorm deals.

Source: Data from Swiss Re

FIGURE 12: ISSUANCE SPREADS VERSUS EXPECTED LOSSES, BY PERIL (H2 2018)



Note: Includes all the bonds issued in the second half of 2018.

Source: Data from Swiss Re

49 Expected loss referenced here is based on the average value of losses over a full range of scenarios, taking into account the attachment and exhaustion points on the bond. This is not the same as the average losses suffered by the full portfolio of referenced insurance policies.

Figure 11 plots the spreads on issuance for the four cyber Cat bonds issued in the final quarter of 2023 against their respective modelled expected loss (red dots), and alongside similar metrics for other selected Cat bonds issued in the same period (other symbols). The data suggest the issuance spreads on the cyber bonds were indeed wider than might be explained solely by differences in expected loss.

Figure 12 shows the comparable chart for the first two dedicated wildfire bonds issued in H2 2018. While the spreads for taking on pure wildfire risks were somewhat wider than bonds with similar modelled expected losses, the deviation is hardly noticeable compared with the average spread-to-expected loss relationship during the same period. This suggests the initial novelty premium was not particularly large for wildfire ILS, perhaps because the underlying drivers of the losses (especially the physical factors that could amplify the hazard) were thought to be relatively well understood, at least at the time.

Source: Geneva Association

The initial cyber Cat bond issuers may have been willing to meet investor demands for a relatively high price of protection on the grounds of establishing an important source of alternative risk capital to support cyber insurance growth. The deals were deliberately structured to be repeatable, perhaps as part of a programme of future issuance. In this sense, the deals may have embedded some additional 'real' option value for the pioneering sponsors that could be realised on future transactions. But 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 more regular cyber ILS.

3.2 Main outstanding obstacles

Besides instrument features and market pricing, the design and execution of the recent cyber ILS also revealed some important underlying challenges. Overcoming these will be important in progressing cyber ILS deals from simply a demonstration of proof of concept to a genuinely enduring and scalable source of risk-absorbing capacity.

3.2.1 Doubts about contract certainty

The proliferation of customised wordings in cyber insurance policies and the knock-on implications for what might lead to losses for a cyber Cat bond, has been and continues to be a major deterrent for investors. Varied qualifying event definitions (i.e. the perils included, temporal limits, damages covered etc.) and different policy exclusions (e.g. for war, critical infrastructure) potentially undermine contract certainty. The triggering events for an insurance claim can be quite wide ranging, from an accidental dissemination of flawed software or an irregular cloud outage to a malicious attack on key third-party service providers. Cyber risks are challenging enough to assess without additional, complicating issues relating to policy wording.

Despite the progress in the industry in tightening up contract language for war and critical infrastructure exclusions, the lack of consensus on policy wordings is unhelpful. In the current hostile environment, cyber is increasingly seen as a weapon that could be used for disruptive/destructive purposes by rogue nation states or cybercriminals. While hostile cyber incidents carried out at the direction or under the control of a sovereign state lie outside of conventional insurance coverage, investors worry about potential coverage disputes that might still arise, especially given the legal uncertainty that persists around attribution.

Variation in policy wording and exclusions in cyber insurance contracts can deter investors from participating in cyber ILS.

As well as the underlying primary policies, reinsurance contract wordings can also create scope for confusion among prospective ILS investors. It may not always be clear how far the losses incurred by the sponsor from a cyber incident extend to non-cyber policies. For instance, while losses arising from disruption to critical infrastructure – which itself is not universally defined by re/insurers – are not covered under standalone cyber insurance, they may indirectly lead to insured claims on other P&C policies.[50] Similarly, a cyber incident may prompt follow-on D&O liability claims against company executives if they failed to implement effective governance.[51]

Arguably, for some types of perils, such as a major cloud outage, these issues are straightforward. For example, as with Nat Cat perils, hours clauses – which define the timeframe over which losses may be cumulated – and occurrence loss limits typically apply. However, other perils like ransomware/malware or phishing attacks are much more

50 CRO Forum 2023.

51 The legal hurdles for establishing a claim against company directors for failing in their oversight responsibilities as regards cybersecurity are significant. Nonetheless, case like the SolarWinds cyberattack in 2020 illustrate the potential additional liability implications for companies that might follow a major incident including securities class actions and regulatory enforcement. See the discussion in LaCroix 2023.

difficult to address if a related loss comes to light only slowly over time. Similarly, coverage triggered by 'system failure' or 'non-malicious' events is not always included in standard cyber insurance, although it can be added through individual policy endorsements and extensions, often with agreed sublimits.[52]

Parametric or index-based contracts might help make contracts clearer but the reference indices for cyber are still developing.

In principle, parametric or index-based contracts might help to increase contract clarity, not least because the triggering event can often be more precisely defined and the need for loss adjustment is less. However, the reference indices for cyber are still nascent and lack a strong track record of relevance and reliability. In the case of industry-wide losses, the limited contract standardisation in standalone cyber insurance adds to the challenges in designing a representative benchmark. In particular, the implicit assumption that war exclusions are the same across jurisdictions could still spur legal challenges.

The important influence of cyber policy wordings on insured losses came into sharp focus following the recent global IT outage caused by a CrowdStrike service update that contained a software flaw which caused 8.5 million Microsoft Windows machines to crash.[53] Although the size of associated ultimate insured losses is unlikely to trigger any of the recently issued cyber Cat bonds, some investors were reportedly unaware that a non-malicious incident might be a qualifying event. Similarly, there was initial uncertainty as to how far business interruption losses insured under non-cyber policies would be treated in the cyber ILS.[54]

3.2.2 Limited market participation and illiquidity

Despite the appeal of a 144A bond format, the investor base for cyber ILS remains narrow, certainly compared with Nat Cat ILS, which itself is much smaller than for mainstream asset classes like equities and bonds. The syndication of the initial cyber Cat bonds was spread over relatively few investors, with most taking up a small allocation compared with a few lead investors on each transaction.[55] Some of the investors were also the third-party ILS investment vehicles of existing reinsurers who were willing to allocate a small amount of their portfolio towards cyber but may not have wanted to invest at scale given their existing cyber insurance portfolios on the liability side of their respective balance sheets.

ILS funds may not have authority from their end-investors to invest in cyber risk, and changing those mandates often involves long lead times, especially if formal approval from the trustees of pension funds or sovereign wealth funds is required. Even if ILS funds have delegated discretion to invest in alternative asset classes, including cyber ILS, they may still be reluctant to take on significant exposure to a new and highly uncertain peril. End-investor trust can be eroded quickly if surprisingly large losses are incurred on an asset class that was not expressly approved, which could prompt unplanned fund redemptions and starve them of vital ongoing capital. For instance, a major loss in cyber for a private credit fund that does not have that as a major part of its mandate carries distinct reputational risk for the fund manager.[56]

ILS funds may not have the mandate to take on cyber risk, or may be reluctant to invest in such a new and uncertain peril.

Moreover, while a 144A bond widens the pool of prospective investors for ILS issuance, this does not mean the secondary market is deep and liquid. Trading in ILS is typically much thinner than in other asset classes. Many ILS investors, especially pension funds and other institutions that invest on behalf of retail investors, have 'buy-and-hold' strategies that mean they (or their asset managers) trade such securities only infrequently when they need to rebalance their portfolios. For these investors, any implicit illiquidity premium embedded in the issuance price boosts the available yield, although they still must be mindful of complying with regulations that specify the types of assets in which they may invest.[57]

In contrast, for some shorter-term institutional investors such as hedge funds (but also some UCITS funds), liquidity considerations can be very important. They need to ensure they can readily exit their positions without materially affecting the price of their assets, should they face large, unexpected requests from clients to withdraw their money.

52 Aon 2024b.
53 The Insurer 2024.
54 Artemis 2024d.
55 Anecdotal evidence indicates perhaps 10–15 or so investors were involved across the recent cyber Cat bond deals. This compares with as many as 30–40 investors for a Nat Cat bond, depending on the size and structure of the deal.
56 Private credit funds raise capital by selling limited partner interests to investors. It may be hard to explain to limited partners when they might not have had any inkling the fund was invested in cyber insurance.
57 ESMA is currently investigating eligibility criteria for ILS under the UCITS directive, and any refinement could have important implications for ILS investors. See ESMA 2024b.

While broker-dealers will usually find willing QIBs to acquire a security should it be offered for sale, the terms of exchange, especially for a novel asset class like cyber ILS with relatively few investors, might not always be favourable to the seller.

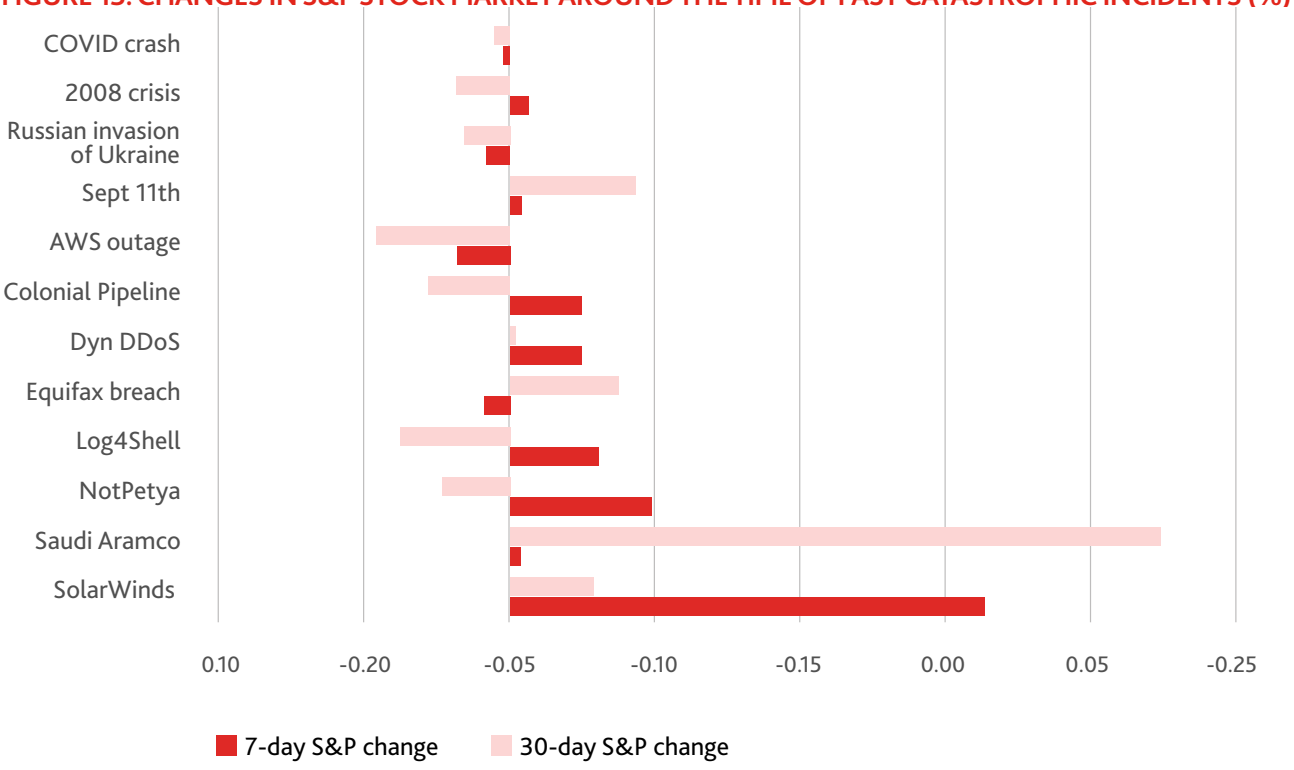
3.2.3 Caution over portfolio diversification benefits

An overriding attraction of Nat Cat ILS for mainstream institutional investors is the diversification benefits such risks provide to their portfolios – i.e. the potential to reduce overall portfolio risk leaving expected returns unchanged or increase the expected return per unit of risk.[58] For some investors, this very often trumps any potential outsized returns. A challenge for cyber ILS, however, is that cyber risk may have systematic features, that by definition cannot be completely diversified away (although the risk may potentially be hedged).[59] That is, cyber incidents have the potential to impact many companies simultaneously, which in extreme cases could also adversely affect their creditworthiness and future earnings, triggering declines in the prices for a wide array of financial assets.

Nat Cat ILS offer diversification benefits, which is attractive to investors. This is more challenging for cyber ILS due to the potential systematic nature of cyber risk.

Previous studies have examined the degree of co-movement between historical cyber incidents and returns on other asset classes. Based on an investigation of stock market performance around the time of past catastrophic incidents, one recent analysis suggests little significant lasting impact of large cyber events on the overall level of equity prices or their perceived riskiness (Figure 13).[60] Further, the spillover effect of past major cyber events appears similar to major hurricanes, perhaps offering scope for analogous potential diversification to that enjoyed by Nat Cat ILS.[61]

FIGURE 13: CHANGES IN S&P STOCK MARKET AROUND THE TIME OF PAST CATASTROPHIC INCIDENTS (%)



Source: Data from Guy Carpenter

However, as explained in Box 6, in the absence of deep knowledge and understanding of the stochastic processes underlying cyber losses (especially the potential for claims from an incident to accumulate across policyholders as well as with other insurance lines), such past correlation metrics may not necessarily be a good guide to future outcomes. Asset markets are forward looking, so how cyber-related losses and returns on other assets covary could be very different according to the constellation of shocks, how investors perceive their effects on future corporate earnings and the degree of persistence.

58 Croco et al. 2014.
59 Several researchers report evidence highlighting the systematic nature of cyber risk. See for example, Jamilov et al. 2023 as well as Freestone and McLelland 2023.
60 Guy Capenter 2023c.
61 Empirical studies generally show that returns on Nat Cat ILS do not tend to move in step with wider financial markets. See discussion in Ahmad 2022.

Box 6: Cyber risks and portfolio diversification

In a world where all asset returns are normally distributed, adding assets with less than perfectly correlated returns provides diversification gains that reduce the overall risk of the portfolio, measured by, for example, value-at-risk (VaR). However, academic studies have shown that this is not necessarily true when returns on assets are not so well behaved in the sense that their distributions cannot be completely described by low-order statistics like mean and variance. For fat-tailed distributions, the tails (the rare events) disproportionately affect the properties of the overall portfolio. Indeed, the work by Ibragimov et al. shows that diversification does not reduce VaR for a large class of dependent, heavy-tailed risks.[62]

In the case of cyber, it seems likely that related insurance claims emanate from probability distributions with heavy/fat tails. This is because:

- Most cyber claims are small but with the potential for rare but outsized losses,
- A serious cyber event may have spillover effects if disruption spreads across digital supply chains or firms are hit by a common disturbance – for instance, a cloud outage,
- The degree of comovement between cyber claims (as well as with other assets) may be stronger during extreme events (i.e. there is stronger dependence in the tail).

Unfortunately, we don't have a rich history of cyber incidents – especially major loss events – to be confident about the 'true' probability distribution for aggregate cyber losses, especially the size and shape of the far-right tail, and how they interact with other assets. Moreover, the dynamic, anthropogenic nature of cyber threats – for example, adversaries and defenders learn and adapt to the shifting threats and vulnerabilities – mean the underlying distribution may not be stable over time. The same outcome from the same stochastic process is not guaranteed at a different time or location.[63]

While the impact of a major Nat Cat disaster on financial markets is often short-lived (in large part the result of a subsequent recovery in physical investment which supports asset prices), the long-run interaction of cyber losses and other asset returns is less clear, especially if such incidents hit companies' reputations and brand values or lead to follow-on mass litigation. At the same time, there are important structural features that limit the potential for cyber-related losses to escalate. For example, major cloud service providers do not operate their architecture in the same way across regions, meaning the potential for international contagion of a cloud outage may be limited.[64] Similarly, the reversible nature of most cyber incidents – most affected systems and data can eventually be restored following a cyber-attack – as well as the potential for risk prevention and mitigation, may cap overall cyber losses.

Re/insurers who assume cyber risks from policyholders, as well as investors in cyber ILS who take the peak risk from re/insurer (or corporate) sponsors, therefore have to take a view about the portfolio diversification opportunities cyber might offer.[65] This includes the potential for future cyber claims to coincide with losses on other insurance perils (intra-risk diversification) and/or occur at the same time as falls in the prices of other assets (inter-risk diversification). Formal models can help but they necessarily rely heavily on expert judgement. Even then, it is impossible to conceive all the possible outcomes that could occur as well as attach meaningful numerical probabilities to all events and/or the magnitude of any consequences.

Source: Geneva Association

Even if some cyber risks are systematic, this need not prevent ILS investors seeking out such exposures if the returns are sufficiently attractive.[66] First, some institutional investors may face lower costs of capital than re/insurers who conversely likely have comparative cost advantages in terms of risk selection, underwriting and claims handling. To the extent that a sponsor of an ILS can achieve capital savings by transferring risk to third-party investors while the latter can benefit from the re/insurer's expertise in underwriting and claims handling, this can form the basis of

62 Ibragimov and Walden 2011.
63 Formally, cyber claims may arise from a non-ergodic stochastic process, where observed past probabilities do not apply to future outcomes. See the discussion in Huggins 2020.
64 Variation in legislation, regulation and litigation relating to data privacy and disclosure matters will also affect the extent of successful liability claims in different jurisdictions. Terry and Brew 2024.
65 Based on interviews with 10 ILS managers, Johansmeyer 2024 reports a range of perspectives on the degree of correlation between cyber risks and financial markets, although the views are often nuanced.
66 If cyber risks are systematic (i.e. there are limited diversification gains from including them in a portfolio), the capital cost advantages ILS investors enjoy might still underpin mutual gains from risk transfer between re/insurers and investors. Indeed, Lakdawalla and Zanjani 2012, show that Cat bonds can mitigate market inefficiencies and improve welfare in the presence of contracting constraints or correlated risks.

mutual gains from the risk exchange.[67] Second, combining cyber and Nat Cat risks might still help balance an ILS investment portfolio, given the likely limited co-dependence between cyber incidents and natural catastrophes. Many Nat Cat events are very unlikely to coincide with insured cyber losses, not least because cyber insurance will typically not pay out for physical damage (although non-affirmative or 'silent' exposures on non-cyber policies might arise).

Furthermore, even though geographical diversification opportunities in cyber are more limited than for Nat Cat perils, extreme cyber incidents might nonetheless impact policyholders differently, depending, for example, on the strength of their cybersecurity or reliance on specific software or hardware. This suggests that cyber ILS can be designed to exploit such intra-risk diversification opportunities, which may be attractive to third-party investors. Consistent with that, a recent study of the four cyber Cat bonds issued in 2023 showed modelled claims that would trigger loss of principal on each of the bonds tend not to be highly correlated.[68]

Some of the traditional risk diversifiers – like industry and geography – are less relevant for cyber, although firms' different use of technology could still be a source of portfolio diversification.

3.3 Near-term market outlook

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.[69] 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.

Given the depth of capital markets, even if mainstream investors only took a very small allocation, the cyber ILS market could expand progressively, in tandem with the primary and reinsurance markets.[70] However, as recently as 2020, only 5% of ILS end-investors were attracted to the idea of investing in securitised cyber risk, reflecting reservations about the complexity of cyber risks and the potential positive correlation between cyber incidents and wider financial market performance. This underscores the task ahead in materially shifting investors' attitude towards the risk.[71]

Such an outlook broadly echoes the path taken for other novel asset classes. The Nat Cat ILS market expanded slowly at first – around USD 1–2 billion per year – and only accelerated from 2005 in the wake of Hurricane Katrina after a major withdrawal of capacity and a sharp rise in reinsurance premium rates that catalysed inflows of alternative capital. Similarly, outside of the insurance sphere, commercial mortgage-backed securities (CMBS) initially developed gradually, taking 10 years to reach a USD 40 billion market, despite a long history of understanding of borrower default risk, the main CMBS risk. Yet if constraints on traditional cyber reinsurance/retrocession do start to bite, this begs the question, what developments might facilitate increased risk-absorbing capacity from financial markets? This is addressed in the next section.

67 Using a stylised model in which firms face different marginal costs in sourcing external capital and providing insurance services (e.g. underwriting and claims management), Boyer and Nice 2012 show how reinsurance is optimally layered, with attachment and exhaustion points varying across different risk protection sellers.

68 Specifically, in a pairwise comparison of the projected losses on two of the four bonds, model simulations suggest investors would suffer a full or partial loss on one or both bonds only around 60% of the time, while investors in one bond would escape any losses altogether when the other bond paid out in full in close to 40% of the modelled outcomes. Baker and Choi 2024.

69 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.

70 According to Prequin, alternative investments will likely reach USD 24.5 trillion by 2028, representing 15% of all assets-under-management. https://www.investmentnews.com/alternatives/news/global-alternatives-market-set-to-reach-24-5t-private-credit-aum-to-double-244679

71 WillisTowersWatson 2020. https://www.globalreinsurance.com/after-big-tests-ils-market-shows-resilience/1435578.article

4 Promoting cyber risk transfer to capital markets

Promoting cyber risk transfer to capital markets

Policy standardisation, improved risk models and re/insurance product innovation will help make cyber ILS more attractive to investors.

Intrinsic uncertainties about future catastrophic cyber losses inevitably act as barriers to full optimal risk sharing. Ambiguity about the scale and likelihood of possible aggregate losses that might accompany a catastrophic cyber event (or series of incidents in quick succession) limits the capital individual carriers can safely and sensibly commit to cyber insurance.

The challenges re/insurers face in quantifying extreme cyber risks are not magicked away by shifting exposures to capital markets, especially if third-party investors are (understandably) nervous of assuming peak cyber risks that re/insurers may be keen to shed. Risk transfer, whether through traditional reinsurance or via new financial vehicles, therefore should be part of a holistic, multi-stakeholder approach to building societal cyber resilience and stronger cybersecurity governance. This includes measures to encourage enhanced risk prevention and mitigation as well as incentivise best-practice cybersecurity among the users and providers of IT hardware, software and associated services.[72]

Nevertheless, ART can almost certainly play a bigger role than hitherto in reallocating cyber risks to those best placed to manage them. The recent cyber ILS transactions demonstrate there is appetite among capital market investors for cyber risk, although 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. Changes to the underlying cyber re/insurance product might also help to promote wider capital market involvement.

Existing investors in ILS typically seek out a quartet of features: ample instrument liquidity, limited correlation with other assets, high expected returns and short duration.[73] Such considerations often underpin the choice to go down the securitised route, and particularly the preference for Cat bonds. This combination of characteristics, however, is not readily achieved for cyber risks. Instead, a broad set of ART solutions, including vehicles that use traditional re/insurance balance sheets to transform risk rather than SPVs, might be most effective in attracting more capital. Different instruments will appeal to a wider base of investors with varied risk preferences, including those who are more comfortable with ambiguity over the size and likelihood of exposures and/or assuming systematic risk.

Attracting greater capital market investment in cyber ILS will require further product innovation from insurers.

The re/insurance sector is already innovating to attract greater third-party capital to support a variety of insurance classes. Some initiatives aim specifically at improving how cyber risks are underwritten and assessed, whether they be backed by traditional or alternative capital. Others look to match capital better against risk on terms acceptable to both protection buyers and sellers. While individually none are likely to unlock a sudden step-up in capacity for peak cyber risks, at least in the near term, collectively they can eventually facilitate more regular cyber risk transfer to capital markets.

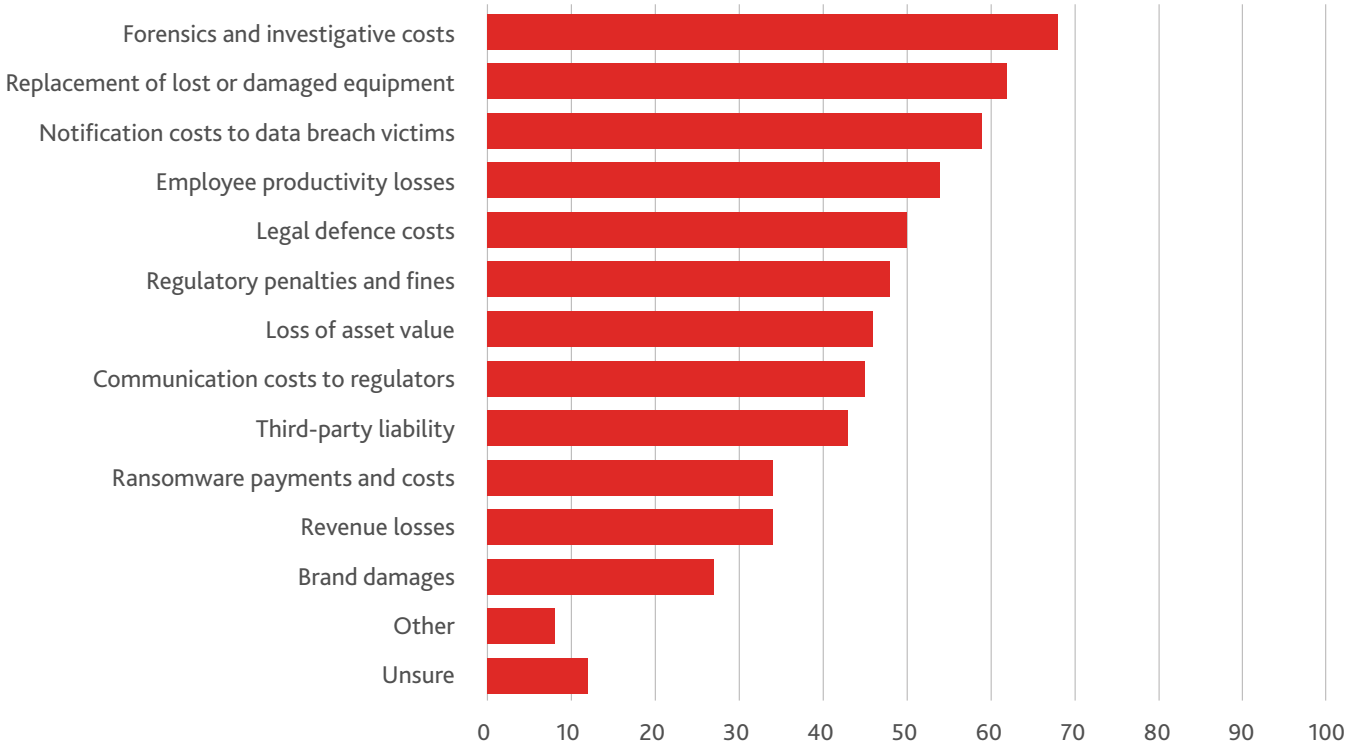
72 For a discussion of various measures that might move societies closer to optimal risk sharing for cyber, see Geneva Association 2023.

73 This point was also highlighted by David Flandro from Howden Tiger during the January 2024 Insurance Insider webinar 'Facing and Overcoming Challenges with Collateralised Reinsurance'.

4.1 Policy standardisation

Although standalone cyber insurance has adapted to meet the expanding needs of firms and households, the extent of coverage still varies widely across policyholders (see Figure 14). For instance, according to a recent global survey by Aon, of the respondents with cyber insurance that cover intellectual property (IP) events, only 36% say the policy protects their own IP assets, 33% say it covers infringement of their IP assets by a third party and 31% say it covers allegations that their company is infringing third-party IP rights.[74] Furthermore, the overall extent of coverage differs markedly, depending on particular policy exclusions, endorsements and extensions. Moves towards policy standardisation could therefore increase contract clarity and improve understanding, including for third-party investors who assume risks from re/insurers.

FIGURE 14: COVERAGE WITHIN CYBER INSURANCE POLICIES IN 2024 (% OF SURVEY RESPONDENTS)



Source: Aon[75]

Some commentators fear that standardisation could itself generate gaps in coverage if it leads to one-size-fits-all policies.[76] They highlight how endorsements and exclusions to basic policies are often themselves already standardised, albeit not necessarily consistently. This means the policy-holder is left to decipher an over- and under-lapping set of documents, all of which may be inappropriate for the risks for which the policyholder is seeking protection and may simply invite disputes over claims if re/insurers' and insureds' respective interpretations of contract terms diverge.

The key therefore is not uniform policies per se, although progress towards market consensus on key exclusion clauses such as war and critical infrastructure would no doubt be helpful, even if legal issues over attribution of cyberattacks to state-sponsored perpetrators persist.

Rather, 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.[77] Such policy language innovation – in both primary insurance policies and associated reinsurance/ILS contracts – would provide a more granular view of the underlying risks. That could help not only third-party investors unfamiliar with cyber insurance, but also re/insurers who could better evaluate their cyber exposures and the associated cost of capital to bear unexpected losses.

Simpler and clearer insurance policy wording would increase contract clarity and reassure third-party investors in cyber risk.

74 Aon 2024b.
75 Aon 2024c.
76 MacTavish 2020.
77 A similar debate arose in the wake of the COVID-19 pandemic and associated legal disputes over the extent of business interruption coverage. See Lloyd's 2020.

Initiatives to promote more objective criteria to define large cyber incidents can support enhanced contract clarity, although these remain nascent. For example, early in 2024 an independent not-for-profit organisation – the Cyber Monitoring Centre (CMC) – was launched in the U.K., tasked with categorising extreme cyber events based on how widespread they are and their financial impact.[78] More recently, Lloyd's and the Association of British Insurers jointly published a framework to help re/insurers define major cyber events.[79] Similarly, ongoing efforts to collect sector-wide insurance claims data (e.g. CyberAcuView) could drive greater consistency in cyber policies and underwriting practices, which in turn should foster more confidence in associated industry loss indices.[80]

4.2 Improved risk modelling

Modelling catastrophic cyber exposure is not as mature as for natural perils. But as highlighted in Box 7, the cyber modelling industry has made significant advances. While there are still notable divergences in model vendors' estimates and version-to-version volatility, the modelled loss metrics have tended to converge over time. Compared with other insurance lines too, the remaining dispersion across models of extreme cyber losses is no wider than for some Nat Cat perils and indeed narrower than for similarly hard-to-predict perils such as terrorism.

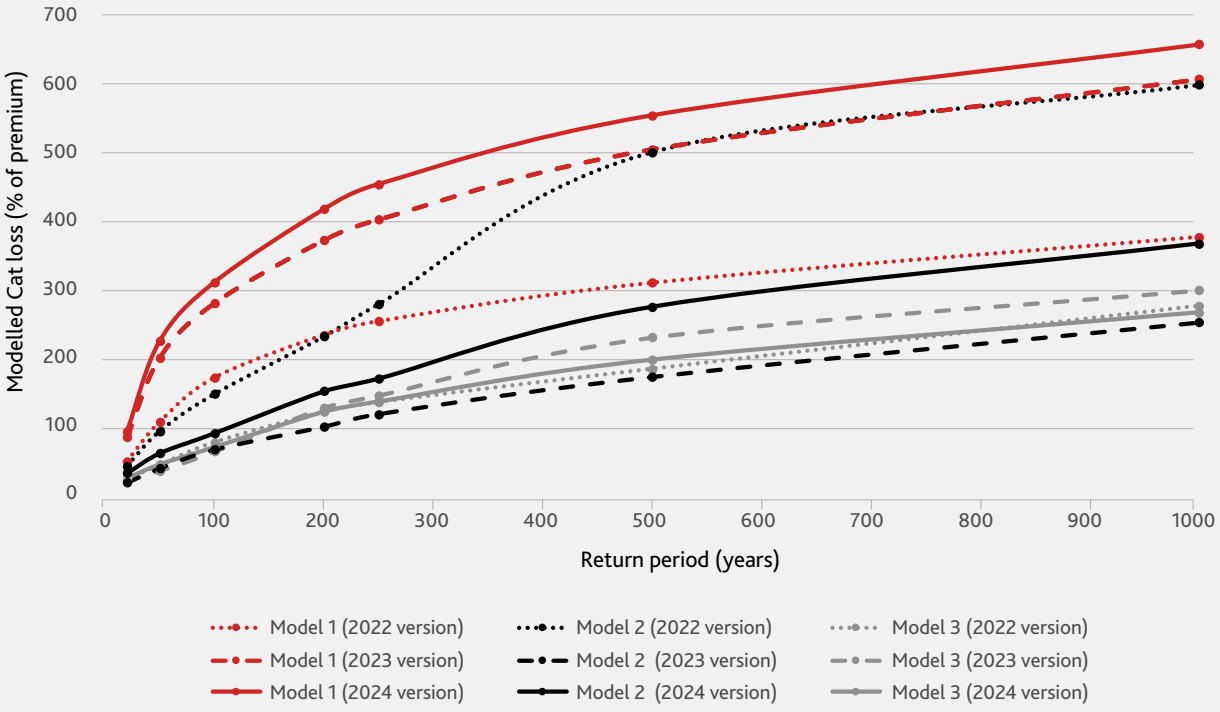
Box 7: Cyber catastrophe modelling – The road to maturity

Cyber catastrophe models are relatively new, having largely only developed over the past decade, with a notable acceleration during the past three years. In that time, the risk assessments of the main model vendors have generally converged as more reliable data have become available to calibrate key parameters that influence the frequency, severity and correlation of estimated cyber losses.[81]

Version-to-version volatility

However, the degree to which modelled loss results align amongst the top three vendors still fluctuates from version to version, especially for extreme tail events. For example, in the latest iteration of modelling (shown in Figure 15), two vendors raised their estimates of ransomware and cloud outage losses in recognition of the worsening cyber threat environment. In contrast, the other main vendor removed some of the highest severity events from its scenario catalogue, resulting in a sizeable fall in estimated tail losses.

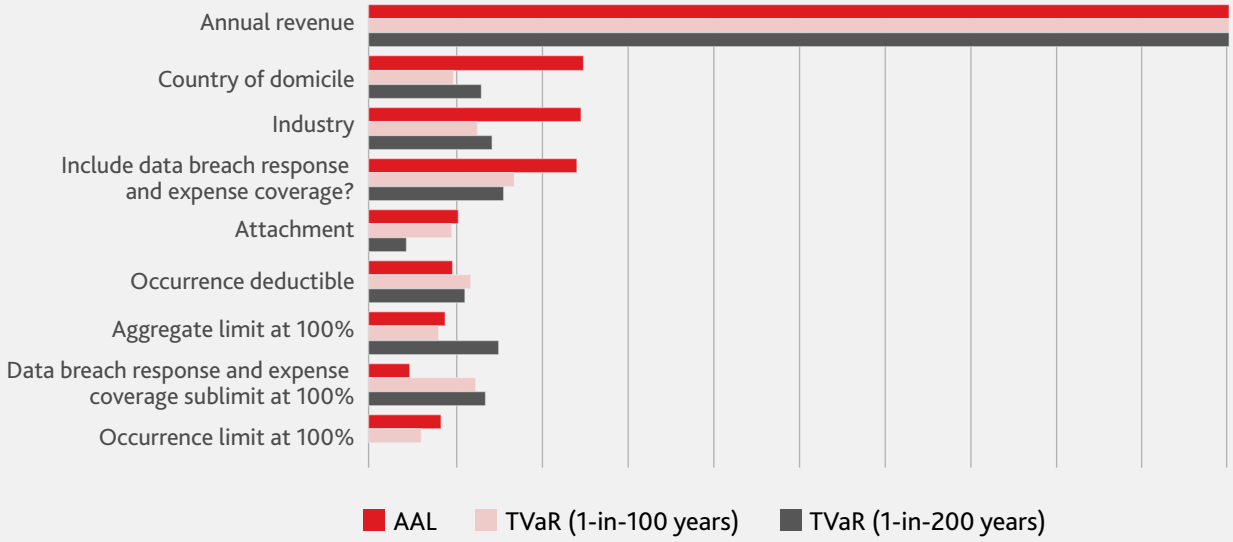
FIGURE 15: MODELLED AGGREGATE LOSS EXCEEDANCE PROBABILITY CURVES



Source: Data from Guy Carpenter

78 See Cyber Monitoring Centre.
79 Lloyd's 2024.
80 See Cyber AcuView.
81 Some early model vintages put implied 1-in-100-year annual U.S. cyber insurance losses at over 550% of total cyber premiums, rising to 620% for a 1-in-200-year event. The latest model versions indicate losses at these respective return periods at less than 300% and 400% of premiums, across all three models. See Guy Carpenter 2019, 2023b.

FIGURE 16: MOST IMPORTANT VARIABLES DRIVING MODEL DISPERSION



Notes:
Figure 15: (i) An exceedance probability (EP) shows the likelihood that a loss of any given size or greater will occur in a given year. (ii) A return period (r) is another way to express the annual EP probability and describes an estimated likelihood of a loss of a given size occurring within a given time frame (i.e. r = 1/EP). (iii) The modelled cyber catastrophe losses were derived using a representative sample of 50,000 cyber policies from Guy Carpenter's GC CyberExplorer® DataLake, which includes over 1 million in-force cyber insurance contracts. Each model simulation was based on the full catalogue of scenarios considered by each vendor, except in the case of CyberCube where 6 infrastructure-related scenarios were excluded. (iv) The estimated losses at different return periods were summed across the sample of policies to derive the aggregate loss EP curve for each of the models.

Figure 16: (i) Bars measure the relative importance of vendor model dispersion. (ii) All variables are scaled to the most important predictor, annual revenue.

Source: Data from Guy Carpenter

Explaining the variation in modelled cyber losses

To examine the issue of model variability further, Guy Carpenter used advanced statistical analysis to interrogate the factors that might explain the divergence in modelled cyber losses.[82] Specifically, for a synthetic portfolio of cyber policies, machine learning algorithms were applied to the outcomes from all three models to uncover any links between the dispersion of simulated losses and characteristics of the insured firm as well its insurance coverage. Separate regressions were estimated for expected modelled losses (average annual loss (AAL)) and more extreme but unlikely losses (measured by tail value-at-risk (TVaR)).[83]

Figure B6 summarises the results. The clear top driver of variability in loss estimates across the three vendors is the size of the insured, with the greatest dispersion concentrated in the nano (less than USD 1 million) and micro (USD 1–5 million) revenue bands. Company scale is often an important proxy for how well it can cope with and recover from a cyberattack, but detailed operational data tends to be less readily available for the smallest firms. Each model vendor therefore relies on their own unique approach to backfill this missing information, leading to divergence in estimated results.

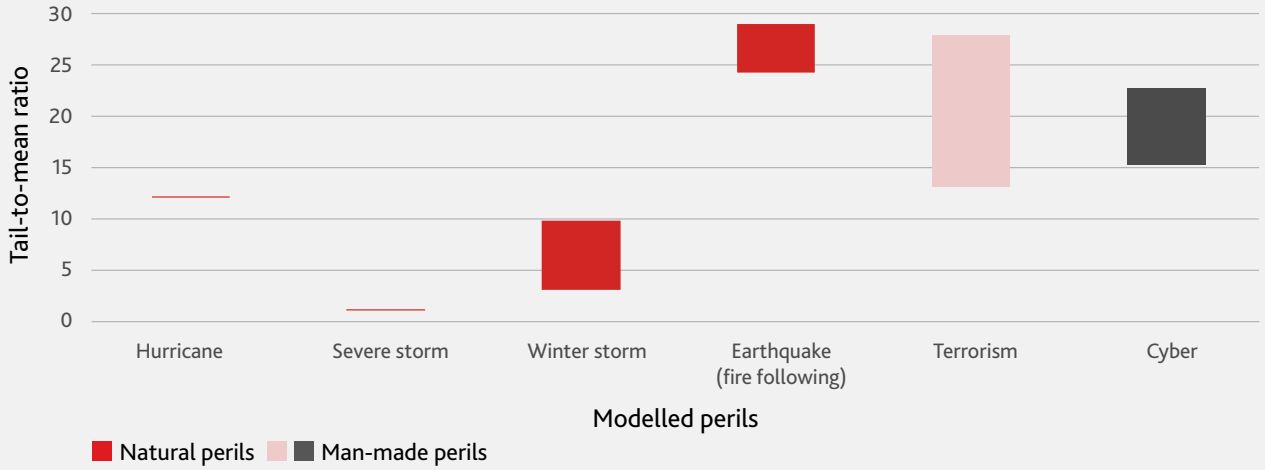
Relative to policyholder characteristics, insurance coverage details appear less important in explaining the variation in modelled losses. Nonetheless, unlike in property insurance, where contract wordings are more homogeneous, cyber policies are written with diverse coverage definitions. As a result, vendor models' distinct treatment of important contractual features such as deductibles and exposure limits do play some role in explaining model dispersion, especially (and unsurprisingly) for extreme losses.

82 Guy Carpenter 2023c, 2024b.
83 The TVaR of a portfolio is defined as the expected loss conditional on the loss exceeding the VaR, which itself refers to the maximum loss over a given period and for a specified degree of confidence. In this way, the TVaR describes the shape of the tail beyond the VaR threshold.

Towards better models

As understanding of cyber risks continues to develop and as more empirical data about the anatomy of cyber incidents (especially major loss events) are captured and analysed, models will undoubtedly improve further. If Nat Cat models are any guide, this will lead to better model calibration and validation, and less dispersion across models. Indeed, despite disparate methodologies, the top three vendors' estimated cyber loss metrics are as, if not more, consistent than models of some more established perils such as earthquakes and terrorism (Figure 17).

FIGURE 17: DISPERSION BETWEEN MODELS, BY SELECTED PERIL



Notes:
(i) The tail-to-mean ratio is calculated by dividing the TVaR for the 1:200 event by the AAL. (ii) The width of the bars indicates the range in the tail-to-mean ratio across the main vendor models for each major peril. (iii) Cyber is based on GC Benchmark portfolio modeled using CyberCube v5.5, Cyence M7 and RMS v8. Nat Cat and terrorism perils are based on the Industry Exposure Database portfolio modelled in RMS RiskLink v23 and AIR Touchstone v10.

Source: Data from Guy Carpenter

Nevertheless, it is important to bear in mind that the range of model projections does not necessarily represent the uncertainty surrounding predictions of future cyber losses – the spread of projected estimates may be too big if it includes the results of unrealistic models and can also be too small if all models are missing the same relevant factor and are therefore similarly biased. Given the field of cyber catastrophe modeling is relatively new, and while the history of extreme cyber incidents remains sparse, the divergence in results is an important reminder of the inherent model uncertainty that exists, and the crucial role expert judgement plays in assessing potential cyber insurance losses.

Source: Contributed by Jess Fung and Shu Iida, Guy Carpenter

As experience of cyber incidents grows, more information will undoubtedly be available to help calibrate the risk of tail events. This will push out the boundaries of insurability and foster appetite for cyber risk both among re/insurers and third-party investors. It may not require a serious cyber catastrophe to resolve some of the uncertainty around such potential extreme but rare events, although the fall-out from major hurricanes in the 1990s no doubt prompted improved quantification of Nat Cat risks.[84] Near misses can also inform about the potential for outsized cyber losses. Specifically, counterfactual analysis – a type of causal reasoning that investigates possible alternative realisations of past events (i.e. what could have happened, but did not) – can illuminate reasonable variations in modelled outcomes.[85]

Ultimately there are some aspects of cyber catastrophes that are simply unmodellable – security in cyberspace is not governed by unchanging scientific or behavioural laws that can be used to predict all future possible outcomes from past experience, at least probabilistically.[86] As a result,

84 Even though Nat Cat models had been used by some re/insurers before the 1990s, the modelling industry enjoyed a major boost in 1992 following Hurricane Andrew. The event illuminated the weaknesses behind simple premium-based risk metrics and encouraged rigorous research into more sophisticated Nat Cat models.

85 For instance, a recent counterfactual investigation of the SolarWinds software supply chain attack assessed that median losses could have amounted to close to USD 20 billion (corresponding to a 1-in-200 year event) had events unfolded differently. Similarly, counterfactual average losses for the WannaCry incident amount to as much as USD 35 billion – equating to roughly a 1-in-1100 return period. This compares with actual insured losses of less than USD 100 million for both incidents. CyberCube 2024b.

86 The advent of artificial intelligence might add a further source of such radical uncertainty given it could fundamentally shift the cyber threat landscape, in potentially unknowable ways.

the contours of the tail of the aggregate loss probability distribution are inevitably very hard to describe and evaluate. This might call for greater transparency and humility in empirical risk modelling in highlighting what is known, what has been assumed and what re/insurers as well as prospective ILS investors simply must take a view on. In turn that might translate into risk metrics about the scale of possible losses that are more expressly imprecise and approximate, but that is a feature not a bug of cyber risk quantification.

Modelling of cyber risks will improve as more historical data on cyber incidents is generated, although certain aspects of cyber catastrophes will remain unmodellable.

To the extent that external vendors provide an independent perspective about potential catastrophic cyber losses, divergence between estimated risk metrics may actually be helpful. Combined with heuristics to help inform their beliefs, re/insurers and third-party investors can (and indeed, do) use the models to interrogate the plausibility of extreme cyber incidents and their tolerance for large, unexpected insurance losses relative to the available rewards. In short, formal models should help inform risk appetite, not dictate asset allocation.

4.3 Re/insurance product development

Apart from better models to quantify potential catastrophic cyber losses, product innovation in re/insurance might also foster capital market involvement in absorbing peak cyber risks. New structures, either in primary cyber insurance policies or associated reinsurance contracts could facilitate the construction of different portfolios of insurance-related risks that better match the appetite and preferred holding periods of investors.

4.3.1 Separate covers for cyber-related perils

Rather than bundle coverage together in an 'all risks' cyber policy, separate covers for different cyber-related perils could be developed. Most obviously, data/privacy breaches and other third-party liability claims might be separated in primary policies from first-party costs like business interruption, or at least isolated in reinsurance arrangements if the end buyer of cyber insurance values the combined product. That more granular cover might appeal to the ILS market, given the potential for adverse loss development (i.e. loss-creep) for longer-tail liability exposures from, for example, data/privacy breaches.[87]

Re/insurance contracts could also be designed explicitly to differentiate coverage for attritional versus catastrophic cyber losses. Such insurance policies already exist in the primary market, most notably in the shape of affirmative cover for events that give rise to major widespread losses – excluding those arising from war or infrastructure impairments – albeit subject to limit and retention levels.[88] But this approach is not universally adopted in all countries, and moreover, may not always dovetail neatly with traditional proportional and aggregate reinsurance structures, which respond to all causes of loss.

4.3.2 Event excess-of-loss reinsurance

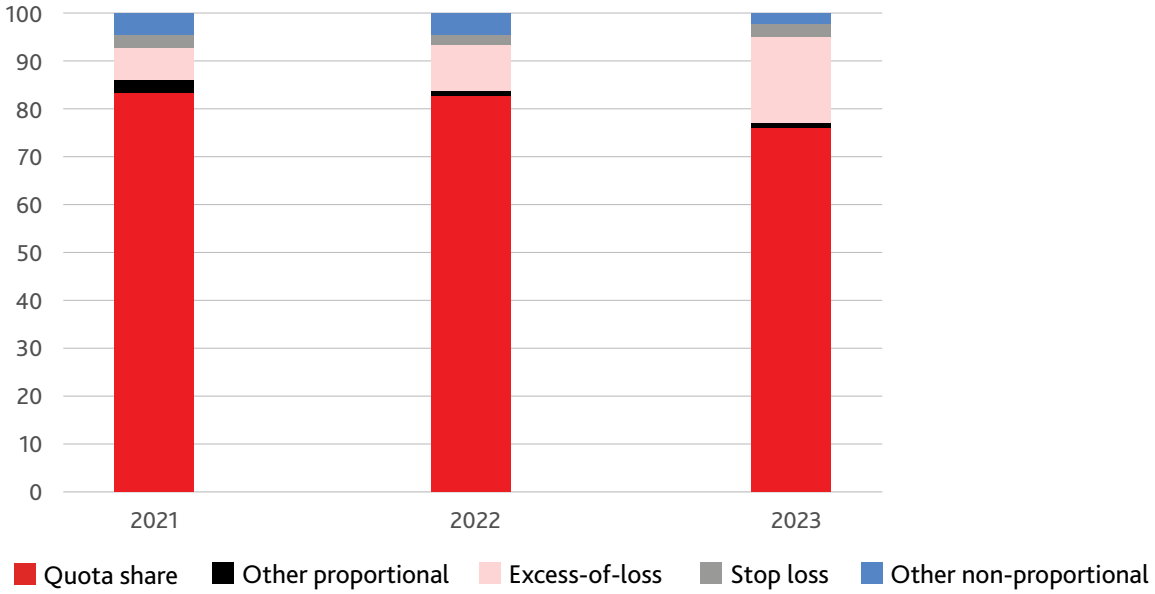
Reinsurers have gravitated mostly to proportional reinsurance structures perhaps due to their own capital requirements. The ceded premiums also help fund the significant investment required to build a robust cyber underwriting process, especially to monitor and manage associated accumulation risks.[89] Some excess-of-loss protection is available in traditional cyber reinsurance markets but it is relatively rare, and what limits are offered tend to be small.[90] In recent renewal rounds, however, reinsurance buying behaviour has selectively shifted toward more targeted excess-of-loss covers (see Figure 18), many of which respond to specifically defined catastrophic scenarios.[91] The foundations for index- and parametric-based reinsurance against extreme cyber incidents also continue to emerge.

The further development of excess-of-loss coverages both in traditional reinsurance and alternative capital markets could also support peak cyber risk transfer.

Further moves in that direction could make it easier to tap traditional as well as alternative capital to reinsure such peak risks, not only through Cat bonds or traditional reinsurance but a wider set of vehicles. And there are signs that such reinsurance innovation is progressing.

87 Claims data for the U.S. indicate an increase in the share of third-party claims suggesting the tail of cyber development may have lengthened in recent years. See discussion in Aon 2024b.
88 See Chubb.
89 American Academy of Actuaries 2021.
90 To the extent that excess-of-loss reinsurance is available, it usually involves aggregate rather than per risk coverage. For example, stop loss reinsurance covers cumulative losses during a specific period (usually 12 months) that exceed either an agreed absolute amount or loss ratio.
91 Guy Carpenter 2024c.

FIGURE 18: SHARE OF CYBER REINSURANCE MARKET, BY POLICY TYPE



Note: Data are based on a survey of global multiline insurers and large reinsurance groups.

Source: Data from S&P Global Ratings

For example:

- Hiscox Re & ILS and Ariel Re recently founded the Cybershock consortium which aims to attract third-party capital to back bespoke, event-focused reinsurance.[92]
- Cyber re/insurance and analytics specialist Envelop Risk launched Envelop SPA 1925, a dedicated cyber reinsurance Special Purpose Arrangement (SPA) at Lloyd's supported by risk capital from a diverse panel of third-party investors.[93]
- Parametrix, a specialist managing general agent (MGA), recently secured a USD 50 million parametric-based cover against cloud outage for a U.S. retailer, with capacity provided by a range of re/insurers.[94]

The complexity and novelty of cyber risks underscore the benefits to investors of partnering with an expert carrier. Furthermore, such ART transactions can economise on collateral if a portion of the tail risk is reassumed by the cedant but without 100% collateral for each dollar of exposure written (sometimes called structural leverage). To the extent that leverage enables the required hurdle rates on cyber ILS to be more readily achieved, this could attract a wider pool of investors and support market pricing that is more attractive to protection buyers.[95] Investors with higher risk appetites like hedge funds and private equity might arguably be more natural marginal investors in peak cyber risks compared with long-term institutional investors like pension funds, especially given the potential systematic nature of the risk.

4.3.3 Innovative collateral release mechanisms

Given that the ultimate insurance loss following a major catastrophic event often takes some time to become established, ILS funds typically set up 'side pockets' to segregate potential loss-impacted contracts from their main portfolios, and use so-called 'buffer loss tables' to determine the pace of collateral release.[96] This provides comfort to the protection buyer that sufficient funds will be available to meet eventual claims that develop only

92 The new entity offers up to USD 50 million in capacity to protect insurers against peak losses from cyber-specific perils such as supply chain disruptions, malware propagation, widespread exploitation of a zero-day software or hardware vulnerability and cloud outages. In doing so, the per occurrence, excess-of-loss reinsurance expressly decouples attritional from catastrophic cyber risks. For more details, see Wallace 2024.

93 Wells 2024a.

94 Artemis 2024e.

95 In a stylised world of perfect capital markets, financial leverage would simply increase the risk of an investment, which ought to be reflected in the cost of capital demanded by investors. This is an illustration of the Modigliani-Miller irrelevance proposition. The (frictional) cost of capital advantages enjoyed by ILS investors might nonetheless underpin the use of leverage to boost their returns on terms that are also acceptable to the cedant.

96 Cedants estimate the eventual value of their loss, with a margin of uncertainty (the 'buffer'). Collateral is withheld to meet claims within that range, while the rest is released to investors. As the ultimate loss value becomes clearer over time, the buffer is reduced.

slowly. For investors, however, collateral can be locked up for extended periods, with no ability to redeploy it elsewhere, thereby restricting returns. It can also complicate the process of attracting additional capital, with ILS funds sometimes choosing to create a new class of shares or a separate SPV to ensure new investors are not exposed to legacy events.[97]

Novel collateral release mechanisms might be especially relevant for cyber where the lags between the reporting and settling of some types of insurance claims can be long. For example, collateral might be released more slowly or apply differently to first-party and third-party liability claims.[98] Rather than commuting a contract, new reinsurance contracts might also be developed to cede the underlying risks and release the withheld claims reserves. Legacy and run-off reinsurance specialist Enstar recently completed the first loss portfolio transfer for prior-year ILS reserves as well as a transaction including an option for ILS investors to exit their positions early, providing illustrations of how such solutions might be organised.[99]

This includes novel collateral release mechanisms or ways for investors to exit their positions before the end of their contractual commitment.

4.4 New investment vehicles and instruments

The prevailing hesitancy among many existing ILS funds for cyber exposure might argue for the development of dedicated ILS funds with explicit cyber investment mandates. Such an approach would allow fund managers to operate within stated and agreed risk tolerances of their clients without having to explain surprisingly good/bad returns on investments that end investors were unsighted about. This might unlock new risk-absorbing capacity, especially if asset managers worry about any unintended cyber exposure they might already have through other P&C policies referenced in existing collateralised reinsurance or sidecar arrangements.[100]

Specialist cyber ILS funds have been mooted before without gaining traction.[101] A challenge is constructing a fund that is sufficiently balanced in the sense that it can exploit any diversification across cyber insurance policies, arising, for example, from the different IT that insureds use.[102] Rather than seeking to hard-wire the diversification benefits within an individual fund, asset managers therefore need to see cyber ILS funds as helping to diversify their overall portfolio. Such a strategy might best suit end investors with a well-developed appetite for alternative assets.

New investment vehicles and instruments, including specialist cyber ILS funds, might unlock new risk-absorbing capacity.

Dedicated cyber ILS funds could also be a part of market initiatives to introduce Exchange Traded Funds (ETFs) that seek access to insurance risks as part of broader investment strategies, distinct from the mutual ILS funds that predominate today.[103] As a marketable security, ETFs trade like equities on a stock exchange and make it possible for retail as well as institutional investors to participate. This enhanced secondary market liquidity could act to widen the investor base in primary ILS markets, including for cyber. Regulators might, however, be uncomfortable with unsophisticated retail investors accessing ILS given the complexity of the associated exposures.

Beyond existing ILS, there may be scope to transfer peak cyber risks directly to capital markets without intermediating them across re/insurers' balance sheets, although such financial innovation remains a distant prospect. Specifically, large industrial companies could issue contingent capital instruments that provide injections of funds in the event of a major cyber incident.[104] No risk is transferred at the time the instrument is issued, but rather the contract gives the issuer the option to raise capital from the protection seller if both counterparties agree that a predefined trigger has occurred.

97 Artemis 2021a.
98 Brew et al. 2023.
99 Artemis 2024c,f.
100 Echoing initiatives by re/insurers, ILS investors have reportedly sought to strip out cyber from other products they invest in, such as property Cat bonds for example. See Artemis 2023b.
101 Artemis 2019b.
102 One analysis based on the SolarWinds incident in 2020 shows that companies from the same location and industry have a higher tendency to use the same third-party service providers and technologies. See KOVRR 2021.
103 Artemis 2024g.
104 For example, a contingent convertible bond (CoCo), also known as an enhanced capital note (ECN), is a fixed-income instrument that is convertible into equity if a pre-specified trigger event occurs.

Some firms already sponsor their own Nat Cat bonds.[105] But unlike those securities, a contingent capital facility need not be fully collateralised, offering investors the chance to boost the available returns (i.e. through synthetic leverage), albeit leaving the corporate sponsor with residual counterparty risk. Aside from inexperience in understanding cyber risks, a constraint for investors could be the concentration among a limited number of sponsors, especially since only a few firms might see value in hedging their extreme cyber exposure. If multiple corporates issued individual cyber-contingent risk financing facilities, this might make it easier for investors to build balanced portfolios, in much the same way that a credit fund invests in a variety of corporate debt instruments from different issuers.

4.5 Digital infrastructure

While not exclusive to cyber, innovations in the way that third-party capital providers are matched with investable opportunities in re/insurance would facilitate risk transfer, whether that be through ILS or other ART solutions. Reducing frictions in the structuring and issuing process will lower transaction costs and broaden the investor base. This includes developments in ILS regulatory regimes that extend the range of available risk management tools and support the introduction of new market infrastructure.[106]

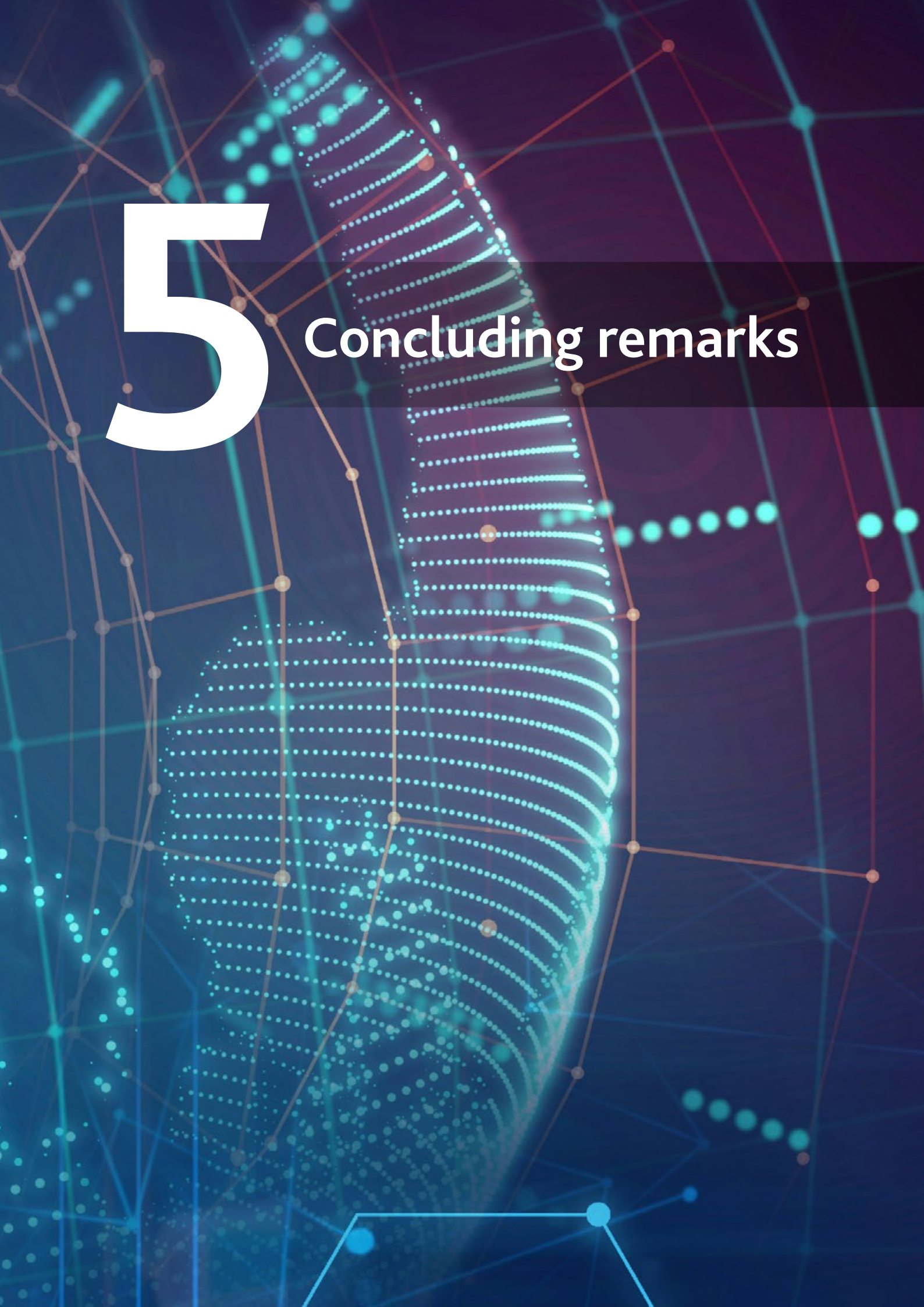
While not exclusive to cyber, digital infrastructure innovations that better match third-party capital providers with investable opportunities in re/insurance would facilitate risk transfer.

As an illustration of the potential in this area, in 2023 CatX successfully raised seed funding for a digital platform to attract alternative capital into the insurance sector, including for cyber index-based and parametric reinsurance and retrocession transactions.[107] Similarly, Lloyd's recently announced extensions to its London Bridge Risk PCC, a transformer vehicle aimed at providing access to insurance risk exposures at Lloyd's, which will enable member companies and managing general agents to source third-party capital to back reinsurance contracts, on both an excess of loss and quota share basis.[108]

As well as improved access to primary capital, new technology can also potentially improve ILS secondary market liquidity. Rather than relying on intermediaries to facilitate the buying and selling of ILS via the over-the-counter market, electronic trading platforms enable investors to transfer and manage risk portfolios digitally in an open market. Though again not restricted to cyber, by providing a marketplace for ILS to be traded, newly established platforms like Akinova aim to enhance the ability of insurers to transfer risk and allow investors to reconfigure and/or fine-tune their portfolios.[109] Schroders and Hannover Re also recently revealed they collaborated on an internal project to tokenise a portfolio of reinsurance contracts (with the tokens tradable on a public blockchain), which if developed further might also be a way to enhance the way ILS assets are invested and managed.[110]

Admittedly, there seems to be limited current demand for active trading of ILS, especially given the significant presence of 'buy-and-hold' investors. The broker-dealer placement model also brings benefits in terms of enabling investors to understand and model what can be complex risks, even if that inevitably introduces additional transaction costs. Nevertheless, if there were deeper more liquid secondary markets for ILS (including for cyber), perhaps more mainstream investors would enter, especially those who need ways to unwind their positions if they face unexpected redemptions from investors. Such enhanced secondary market trading would also help illuminate investors' views about extreme cyber uncertainties and, in turn, aid price discovery about the underlying risks and rewards.

105 A captive insurance company (or a fronting insurer) often acts as an intermediary between the corporate sponsor and capital market investors. For example, Google and its holding company parent Alphabet, issues a regular Cat bond programme to protect itself against California earthquake risks.
106 Several countries have actively sought to develop regulatory frameworks that foster ILS issuance, albeit sometimes with mixed success. Most recently, the U.K.'s Prudential Regulation Authority announced it is liaising with the industry about a new, accelerated pathway for catastrophe bond applications. See Artemis 2024h.
107 Wells 2024b.
108 Lloyd's.
109 Akinova is an independent electronic marketplace for the transfer and trading of re/insurance risk which is regulated in Bermuda. See: https://akinova.com/
110 Ledger Insights 2024.



5 Concluding remarks

Concluding remarks

ART solutions for cyber will gain in importance as exposures grow. Recent developments in the cyber ILS market are promising but broader innovations are needed to transfer peak cyber risks to those best placed to absorb them.

The market for cyber insurance has grown rapidly over a relatively short period of time, both in the scale and scope of coverage. Maintaining that degree of upward momentum to keep up with and ideally outpace rising risk exposures will likely require additional capital resources from outside the re/insurance sector. This is not least because of the uncertainties that persist about the systematic nature of the exposure and the potential for large accumulated insured losses. Such worries restrain the balance sheet capacity of traditional re/insurance carriers, especially incumbent reinsurers that ultimately bear much of the tail risk given the concentration in the market and limited retrocession opportunities.

The recent flurry of cyber Cat bond issues is therefore a welcome development. While the sizes of the individual deals were relatively small, they show the art of the possible in terms of risk transfer. At the same time, important obstacles remain that limit how far and how fast cyber ILS issuance will likely proceed, at least on terms that are mutually attractive to both ILS sponsors and investors. This means the cyber ILS market is most likely to expand only gradually over time, echoing early developments in Nat Cat ILS.

The recent cyber Cat bonds are an important milestone in the development of the cyber insurance market.

Some of the headwinds will no doubt subside as overall knowledge and understanding of catastrophic cyber risks build, both among re/insurers and third-party capital providers. Product innovation includes simpler and clearer re/insurance contract language, granular coverages that better match investor risk preferences and improvements in formal risk quantification, all of which will boost confidence in the potential scale of transferred insurance losses and the possible diversification benefits cyber might offer investors' portfolios. Similarly, initiatives that increase the tradability of ILS as an asset class and thereby boost secondary market liquidity, such as new investment products and market infrastructure could also widen the investor base for cyber ILS.

But expanding capital market involvement will likely require broader solutions than ILS, including those that use rated re/insurance balance sheets to transform cyber risks into investable propositions.

Moreover, capital market involvement in assuming peak cyber risks should not be seen solely through the lens of ILS, many of which developed for Nat Cat perils that do not share the same risk profile as cyber. Broader ART solutions can also play a role, including vehicles that use traditional re/insurance balance sheets (rather than SPVs) to transform cyber risks into investable propositions or perhaps even instruments that allow corporates to shed extreme cyber risks directly to capital markets. This in turn will allow more efficient use of capital and facilitate progress towards more optimal sharing of complex insurance risks like cyber.

The ongoing digitalisation of societies will only increase the importance of cyber as a risk class, and the re/insurance sector and capital market investors must lean in to support the development of ways to transfer cyber risks faced by firms/households to entities better placed to absorb them. The re/insurance sector is actively pursuing such innovation, although progress is likely to remain gradual, as re/insurers and investors alike cautiously navigate the boundaries of insurability in cyber, which themselves move over time.

References

Ahmad, Z. 2022. Insurance-Linked Securities: Diversification and returns. *Schroders*. https://www.schroders.com/en-us/us/intermediary/insights/insurance-linked-securities-diversification-and-returns/

Allianz 2024a. *Risk Barometer 2024*. https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Allianz 2024b. *Global Insurance Report 2024*. 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

Amici, E., and R. Dell'Amore. 2024. ILS Universe Overview. *SIGLO*. https://mcusercontent.com/3c39a63e-2c80a1504afac3197/files/c8724b70-44c4-bd49-94ca-db190a096a82/ILS_Universe_Paper.pdf

Aon. 2023. *Insurance-Linked Securities Aon Securities Q4 2023 Quarterly Report*. https://www.aon.com/reinsurance/getmedia/534d6b61-901b-4652-8095-d51d65699086/20240214-ils-quarterly-report-2023-q4.pdf?utm_source=slipcase&utm_medium=affiliate&utm_campaign=slipcase

Aon 2024a. *Crowdstrike/Windows Event Briefing: Implications for Cyber Re/Insurers: Initial Findings*.

Aon. 2024b. *U.S. Cyber Market Update*.https://www.aon.com/reinsurance/getmedia/4afa8654-6534-48c3-91c1-b27d-57170cdb/20240806-US-Cyber-Market-Update.pdf

Aon. 2024c. *Intangible Versus Tangible Risks Comparison Report: De-risking AI, IP, and Cyber*. https://www.aon.com/en/insights/reports/2024-intangible-versus-tangible-risks-comparison-report

Artemis. 2016. Operational Re, Credit Suisse's Op-risk Cat Bond, Settles at CHF220m. https://www.artemis.bm/news/operational-re-credit-suisses-op-risk-cat-bond-settles-at-chf220m/

Artemis. 2019a. Alternative Capital Now 4% of $2 Trillion Non-life Insurance Market: Swiss Re. https://www.artemis.bm/news/alternative-capital-now-4-of-2-trillion-non-life-insurance-market-swiss-re/

Artemis. 2019b. Hiscox Has Cyber ILS Fund Ambitions. https://www.artemis.bm/news/hiscox-has-cyber-ils-fund-ambitions/

Artemis. 2021a. ILS Fund Side Pocket Strategies Evolving for the Better: Horseshoe's Desmond https://www.artemis.bm/news/ils-fund-side-pocket-strategies-evolving-for-the-better-horseshoes-desmond/

Artemis. 2021b. ILS Fund Side Pocket Strategies Evolving for the Better: Horseshoe's Desmond. https://www.artemis.bm/news/ils-fund-side-pocket-strategies-evolving-for-the-better-horseshoes-desmond/

Artemis. 2023a. Cyber Reinsurance, Retro & ILS All Critical to Market Expansion: S&P. https://www.artemis.bm/news/cyber-reinsurance-retro-ils-all-critical-to-market-expansion-sp/

Artemis 2023b. Cyber ILS Will See a Different Distribution of Capital: Gallagher Re's Newman & Norris. https://www.artemis.bm/news/cyber-ils-will-see-a-different-distribution-of-capital-gallagher-res-newman-norris/

Artemis. 2023b. Cyber Catastrophe Could Deter ILS Investors: Conning. https://www.artemis.bm/news/cyber-catastrophe-could-deter-ils-investors-conning/

Artemis. 2024a. *Q1 2024 Catastrophe Bond & ILS Market Report*. https://www.applebyglobal.com/wp-content/uploads/catastrophe-bond-ils-market-report-q1-2024.pdf

Artemis. 2024b. Beazley Sponsors Further $160m Cyber Cat Bond via PoleStar Re, Takes Total to $300m.
https://www.artemis.bm/news/beazley-sponsors-further-160m-cyber-cat-bond-via-polestar-re-takes-total-to-300m/

Artemis. 2024c. Enstar $350m ILS Legacy Deal Included COVID-19 Exposures, Expands its Run-off Portfolio.
https://www.artemis.bm/news/enstar-350m-ils-legacy-deal-included-covid-19-exposures-expands-its-run-off-portfolio/

Artemis. 2024d. CrowdStrike Outage: Cyber cat bond prices stable, uncertainty palpable.
https://www.artemis.bm/news/crowdstrike-outage-cyber-cat-bond-price-stable-uncertainty-palpable/

Artemis. 2024e. $50m Parametric Cloud Outage Cyber Cover Secured for US Retailer by Parametrix.
https://www.artemis.bm/news/50m-parametric-cloud-outage-cyber-cover-secured-for-us-retailer-by-parametrix/

Artemis. 2024f. Forward Exit Option (FEO) – A flexible finality solution for ILS investors: Zaprianov, Enstar.
https://www.artemis.bm/news/forward-exit-option-feo-a-flexible-finality-solution-for-ils-investors-zaprianov-enstar/

Artemis. 2024g. Brookmont to Launch Exchange-traded Cat Bond Fund, Catastrophic Bond ETF.
https://www.artemis.bm/news/brookmont-launch-exchange-traded-cat-bond-fund-catastrophic-bond-etf/

Artemis. 2024h. UK PRA to Consult on ISPV Reforms, Launch Accelerated Catastrophe Bond Pathway.
https://www.artemis.bm/news/uk-pra-to-consult-on-ispv-reforms-launch-accelerated-catastrophe-bond-pathway/

Artemis. 2024i. Beazley Gets New PoleStar Re 2024-3 Cyber Cat Bond with Further Upsize to $210m.
https://www.artemis.bm/news/beazley-gets-new-polestar-re-2024-3-cyber-cat-bond-with-further-upsize-to-210m/

Baker, B., and J. Choi. 2024. Digital Ties and Natural Divides: Correlation and diversification in cyber catastrophe bonds. *CyberCube*. https://insights.cybcube.com/correlation-and-diversification-in-cyber-catastrophe-bonds

Balalaeva, I. 2024. Rule 144A.
https://cbonds.com/glossary/rule-144a/

Beazley. 2024. Beazley Closes $140m Cyber Catastrophe Bond.
https://www.beazley.com/en-CA/news-and-events/beazley-closes-$140m-cyber-catastrophe-bond/

BeInsure. 2024. *Primary & Secondary ILS Market Quarterly Review.*
https://beinsure.com/primary-secondary-ils-market-review/

Boyer, M., and C. Nice. 2012. An Industrial Organization Theory of Risk Sharing. *North American Actuarial Journal* 17 (4): 283–296. https://www.tandfonline.com/doi/abs/10.1080/10920277.2013.839377

Braun, A., M. Eling, and C. Jaenicke. 2023. Cyber Insurance-linked Securities. *ASTIN Bulletin* 53 (3).
https://www.cambridge.org/core/journals/astin-bulletin-journal-of-the-iaa/article/cyber-insurancelinked-securities/69986C0DCA02746A0FBD678042A44D67

Brew, O., Z. Breslin, D. Ross, D, B. Baker, and Y. Essen. 2023. Unlocking Potential – Why now is the time cyber ILS has the momentum to succeed. *Lockton Re.*
https://assets.ctfassets.net/zr7mmeciv2ps/5Q7LxCdFrvRGwxLypzKrmt/f9eb3ca81e7a0be11f9e49a9e3339954/Feb23UnlockingPotential.pdf

Coalition 2022. Coalition and BDT Capital Partners Announce the Launch of Ferian Re.
https://www.coalitioninc.com/announcements/coalition-and-bdt-capital-partners-announce-the-launch-of-ferian-re

Croco, R., R. Guinn, and T. Robinson. 2014. The Free Lunch Effect: The value of decoupling diversification and risk. *Salient*. https://www.advisorselect.com/transcript/the-free-lunch-effect-the-value-of-decoupling-diversification-and-risk-august-2014/the-free-lunch-effect-the-value-of-decoupling-diversification-and-risk-august-2014

CRO Forum. 2023. *Breaking Point: Critical infrastructures disrupted.* https://www.thecroforum.org/wp-content/uploads/2023/11/Breaking-Point_Critical-Infrastructure-Disrupted.pdf

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

CyberCube. 2024b. Three Degrees of Separation: Understanding cyber tail risk with counterfactual analysis. https://insights.cybcube.com/three-degrees-of-separation-cyber-tail-risk-report

Davis, D., and J. Clark. 2020. Private Insurance Linked Securities. *Frontier Advisors*. https://www.frontieradvisors.com.au/wp-content/uploads/2020/11/Frontier-Line-169-Private-insurance-linked-securities.pdf

DiFiore, P. 2019 Diversifying into Insurance Risk Premia. *Neuberger Berman.* https://www.nb.com/en/global/insights/diversifying-into-insurance-risk-premium

Edmonds, C. 2015. Fronted Reinsurance and Northern Rock – What do they have in common? *Soldium.* https://solidumpartners.ch/en/blog-posts/fronted-reinsurance-and-northern-rock-what-do-they-have-common

ESMA. 2024a. *Consultation Paper: Draft regulatory technical standards on liquidity management tools under the AIFMD and UCITS Directive.* https://www.esma.europa.eu/sites/default/files/2024-07/ESMA34-1985693317-1095_CP_on_RTS_on_LMTs_under_AIFMD_and_UCITS_Directive.pdf

ESMA. 2024b. ESMA Asks for Input on Assets Eligible for UCITS. https://www.esma.europa.eu/press-news/esma-news/esma-asks-input-assets-eligible-ucits

Freestone, T., and M. McLelland. 2023. Cyber Risk's Fundamental Mischaracterisation As an Insurance Risk. *InsuranceERM.* https://www.insuranceerm.com/analysis/cyber-risks-fundamental-mischaracterisation-as-an-insurance-risk.html

Gallagher Re. 2022. *CY–FI: The future of cyber (re)insurance.* https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/future-of-cyber-reinsurance.pdf

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

Geneva Association 2023. Cyber Risk Accumulation: Fully tackling the insurability challenge. Author: Darren Pain. https://www.genevaassociation.org/publication/cyber/cyber-risk-accumulation-fully-tackling-insurability-challenge

GFIA. 2023. *Global Protection Gaps and Recommendations for Bridging Them.* https://gfiainsurance.org/news/493/new-report-identifies-trillion-dollar-global-protection-gaps

Guy Carpenter. 2019. *Looking Beyond the Clouds: A U.S. cyber insurance industry catastrophe loss study.* https://www.guycarp.com/insights/2019/09/guy-carpenter-and-cybercube-report-reveals-potential-impact-of-cyber-catastrophe-scenarios-on-u-s-cyber-insurance-industry.html

Guy Carpenter. 2023a. *Double-Whammy? Examining the correlation between major cyber events and broad market performance.* https://www.guycarp.com/insights/2023/09/double-whammy-examining-correlation-between-major-cyber-events-broad-market-performance.html

Guy Carpenter. 2023b. *Through the Looking Glass: Interrogating the key numbers behind today's cyber market.* https://www.guycarp.com/content/dam/guycarp-rebrand/pdf/Insights/2023/Guy_Carpenter_Cyber_(Re)insurance_Market_Report_Publish_rev%20.pdf

Guy Carpenter. 2023c. *Under the Lens: Investigating cyber vendor model divergence.* https://www.guycarp.com/insights/2023/06/under-the-lens-investigating-cyber-vendor-model-divergence.html

Guy Carpenter. 2024a. A Closer Look: Unveiling the global impact of CrowdStrike event. https://www.guycarp.com/insights/2024/07/global-outage-with-widespread-impact.html

Guy Carpenter. 2024b. *Refocusing the Lens: An updated look at cyber model divergence.* https://www.guycarp.com/insights/2024/03/refocusing-the-lens-updated-look-cyber-model-divergence.html

Guy Carpenter. 2024c. A Global Outage with Widespread Impact. https://www.guycarp.com/content/dam/guycarp-rebrand/insights-images/2024/07/2024_7_Cyber_event_analysis_published.pdf

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

Howden. 2024b. *How Does Reinsurance Affect the Cyber Insurance Market for Buyers?* https://www.howdengroup.com/uk-en/how-does-reinsurance-affect-the-cyber-insurance-market-for-buyers

Huggins, P. 2020. https://medium.com/@oracuk/this-phrase-is-interesting-and-i-think-opens-up-a-world-of-debate-about-cyber-risk-d94033872b1c

Ibragimov, R., and J. Walden. 2011. Value at Risk and Efficiency under Dependence and Heavy-tailedness: Models with common shocks. *Annals of Finance* 7: 285–318. https://scholar.harvard.edu/files/ibragimov/files/value_at_risk_under_dependence_and_heavy-tailedness_models_with_common_shocks.pdf

Jamilov, R., H. Rey, and A. Tahoun. 2023. The Anatomy of Cyber Risk. *Institute for New Economic Thinking Working Paper Series No. 206*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4470871

Johansmeyer, T., and A. Mican. 2022. Cyber ILS: How acute demand could drive a scalable retro market. *The Journal of Risk Management and Insurance* 26: 1. https://jrmi.au.edu/index.php/jrmi/article/view/245

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

Johansmeyer, T. 2024. Perception Shapes Reality: How views on financial market correlation affect capital availability for cyber insurance. *The Journal of Risk Management and Insurance* 28: 1. https://jrmi.au.edu/index.php/jrmi/article/view/287

King & Spalding. 2022. *Considerations for Hybrid Rule 144A and 4(a)(2) Transactions.* https://www.kslaw.com/attachments/000/010/070/original/Considerations_for_Hybrid_Rule_144A_and_4%28a%29%282%29_Transactions.pdf?1667848364

KOVRR. 2021. Cyber Risk Aggregation Case Study: SolarWinds. https://www.kovrr.com/case-studies/cyber-risk-aggregation-case-study-solarwinds

LaCroix, K. 2023. SEC Files Cybersecurity Disclosure Suit Against SolarWinds and Exec. *D&O Diary*.
https://www.dandodiary.com/2023/10/articles/cyber-liability/sec-files-cybersecurity-disclosure-suit-against-solar-winds-and-exec/

Lakdawalla, D., and G. Zanjani. 2012. Catastrophe Bonds, Reinsurance, and the Optimal Collateralization of Risk Transfer. *Journal of Risk and Insurance* 79: 2.
https://onlinelibrary.wiley.com/doi/10.1111/j.1539-6975.2011.01425.x

Ledger Insights. 2024. Schroders Capital, Hannover Re in ILS Tokenization Trial.
https://www.ledgerinsights.com/schroders-capital-hannover-re-in-ils-tokenization-trial/

Linna, L. 2023. Alternative Investments Industry "Expected to Show Solid Growth": Preqin. *Delano.*
https://delano.lu/article/preqin-alts-2028-report-indust.

Lloyd's. 2020. *Building Simpler Insurance Products to Better Protect Customers: The insurance industry response to COVID-19*.
https://assets.lloyds.com/assets/lloyds-product-simplification-report-final/1/Lloyds_product_simplification_report_FINAL.pdf

Lloyd's. 2024. *Components of a Major Cyber Event: A (re)insurance approach.*
https://www.lloyds.com/about-lloyds/our-market/what-we-insure/cyber/components-of-a-major-cyber-event

MacTavish. 2020. Manufacturing Confusion: *The dangers of standardised policy wordings.*
https://www.mactavishgroup.com/insights/policy-standardisation-report

Njegomir, V., and R. Maksimović. 2009. Risk Transfer Solutions for the Insurance Industry. *Economic Annals* LIV: 180.
https://pdfs.semanticscholar.org/c1a8/bfeb52f43dc8d11bdbb46fd5544393cf3775.pdf

Reinsurance News. 2024. Global Reinsurer Capital Up 17% to $670bn in 2023: Aon.
https://www.reinsurancene.ws/global-reinsurer-capital-up-17-to-670bn-in-2023-aon/

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

Swiss Re. 2024. *Insurance-Linked Securities Market Insights Edition XXXV*.
https://www.swissre.com/dam/jcr:bb189e59-a15f-49df-a250-07b2c6b2d9bd/2024-02-sr-ILS-market-insights-feb-2024.pdf

Terry, A., and O. Brew. H1 2024 Cyber Reinsurance Update. *Lockton Re.*
https://assets.ctfassets.net/zr7mmeciv2ps/1sjOkvoLlle97OI6seusCn/d3b827740c5fac587b7d911e024bec42/H1_2024_Cyber_Reinsurance_Update_FINAL.pdf

The Insurer. 2024. Ariel Re's Carr: CrowdStrike highlights cyber coverage discrepancy concerns.
https://www.theinsurer.com/reinsurancemonth/ariel-res-carr-crowdstrike-highlights-cyber-coverage-discrepancy-concerns/

Verisk. 2024. *Everything You Need to Know about PCS.*
https://www.verisk.com/4a5267/siteassets/media/pcs/pcs-consolidated-methodology-paper.pdf

Wallace, M. 2024. Hiscox Re Goes Behind the Scenes of its Cyber Catastrophe Consortium. *ReInsurance Business.*
https://www.insurancebusinessmag.com/uk/news/reinsurance/hiscox-re-goes-behind-the-scenes-of-its-cyber-catastrophe-consortium-491877.aspx

Wells, K. 2024a. Envelop Risk Launches Dedicated Cyber Reinsurance Lloyd's Vehicle with Apollo. *Reinsurance News.*
https://www.reinsurancene.ws/envelop-risk-launches-dedicated-cyber-reinsurance-lloyds-vehicle-with-apollo/

Wells, K. 2024b. CatX Partners with CyberCube to Enhance its Cyber Capabilities. *Reinsurance News.* https://www.reinsurancene.ws/catx-partners-with-cybercube-to-enhance-its-cyber-capabilities/

WillisTowersWatson. 2020. After Big Tests, ILS Market Shows Resilience: 2020 Global Insurance-Linked Securities Market Survey Report. *Global [Re]Insurance.* https://www.globalreinsurance.com/after-big-tests-ils-market-shows-resilience/1435578.article

Wright, A. 2024. Insurance-Linked Securities and Collateral: An essential overview. *Captive.com.* https://www.captive.com/articles/insurance-linked-securities-and-collateral-an-essential-overview+

The Geneva Association
Talstrasse 70
Zurich, Switzerland

www.genevaassociation.org