Projecting Cyber Insurance Growth: A 10-Year US Market Outlook

CyberCube

Quantifying growth from all sides

The property & casualty (P&C) insurance sector stands at the threshold of a once-in-a-generation opportunity to build a sustainable market for cyber risk transfer. This enables societal resilience to one of the peak risks facing economies today. There is little controversy in the statement that the cyber insurance market is set for outsized growth compared with other lines of P&C insurance over the coming 10 years. There is some concern, however, about what factors must come together for this growth to be achieved — especially in light of slow-to-declining premium numbers for the US standalone market in FY2023[1].

At CyberCube, we provide the world's leading analytics to quantify cyber risk. In this report, we apply our quantification lens to the growth trajectory of the US standalone cyber market in the next 10 years, from 2024 to 2034. We have stress-tested premium growth numbers, overlaid capital requirements to support the growing line of business, and asked what structural changes would be required to meet the projections.

Our key findings are:

1. Cyber insurance is projected to grow rapidly over the next decade, driven by increasing digitization of the global economy and rising concerns about cyber risk. CyberCube has modeled three compound annual growth rate (CAGR) factors for the US insurance industry to 2034: 10% growth resulting in $17 bn of premium; 20% growth resulting in $45 bn of premium and 30% growth resulting in $109 bn of US cyber premium.

2. Cyber will become a peak peril, with the potential for losses from US Standalone Cyber to exceed Hurricane Katrina — the largest insurable natural catastrophe to date. At 20% CAGR, the amount of capital required to manage a 1-in-250 year loss would be $121 bn. Hurricane Katrina, for example, cost the (re)insurance industry $102 bn in 2005.

3. The (re)insurance market will need to substantially increase cyber's capital allocation to enable this growth potential, with increases needed from multiple sources including insurers, reinsurers, capital markets, and potentially private-public partnerships.

(All values are in 2023 dollars)

1. https://www.fitchratings.com/research/insurance/us-cyber-insurance-maintains-strong-profits-premium-growth-slows-16-04-2024

While CyberCube acknowledges that there is significant uncertainty in undertaking a 10-year projection study and this research requires making simplifying assumptions (see panel "**A 10-year view: projection assumptions**"), our intent with this paper is threefold:

- To spark a more quantified conversation around the implications of the various growth assumptions for the cyber insurance market.
- To estimate the capital management strategies that will be required to sustain the projected rapid market growth and explore the potential sources of that capital.
- To uncover additional areas of structural change that may impact the market's ability to meet the increasing demand. These areas may be expanded on in future CyberCube analysis.

A huge opportunity with rising capital intensity:

Market leaders conclude that cyber insurance is poised for exponential growth over the coming decade, but it remains a capital-intensive peril that requires structural innovation to meet the rising demand and foster resilience for society. CyberCube's US Industry Exposure Database (IED)[2] pegs US standalone premium in 2023 at $8 bn. Assuming all risk carriers manage capital against their exposures to a 1-in-250 year aggregate loss event, CyberCube's *Portfolio Manager*[3] catastrophe model estimates that the industry required $20 bn of capital in 2023. In other words, (re)insurers need $20 bn to meet obligations for a 1-250 year (0.4% probability) cyber aggregation loss.

A 10-year view: projection assumptions

- Estimates are for US Standalone business only, using CyberCube's Industry Exposure Database. All projections have a high range of uncertainty. We considered three scenarios: CAGR of 10%, 20%, or 30%.
- Exposure grows proportionally to premium. If the industry manages to a certain loss ratio, premium should be a guide for exposure and losses. This exercise was not intended to project the future composition of the insurance market (e.g. adoption rates by size/industry and limits purchased).
- Changes in the cyber threat landscape do not fundamentally alter the frequency or severity of attacks. Evolutions in offensive and defensive strategy and tactics (e.g. innovations in artificial intelligence or quantum computing) could emerge to fundamentally shift projections.
- All values are in 2023 USD.
- Capital continues to be managed to 1-in-250 cat event, resulting in a $20 bn capital base in 2023 for the estimated $8 bn of US standalone premium, based on CyberCube's Portfolio Manager cat model.

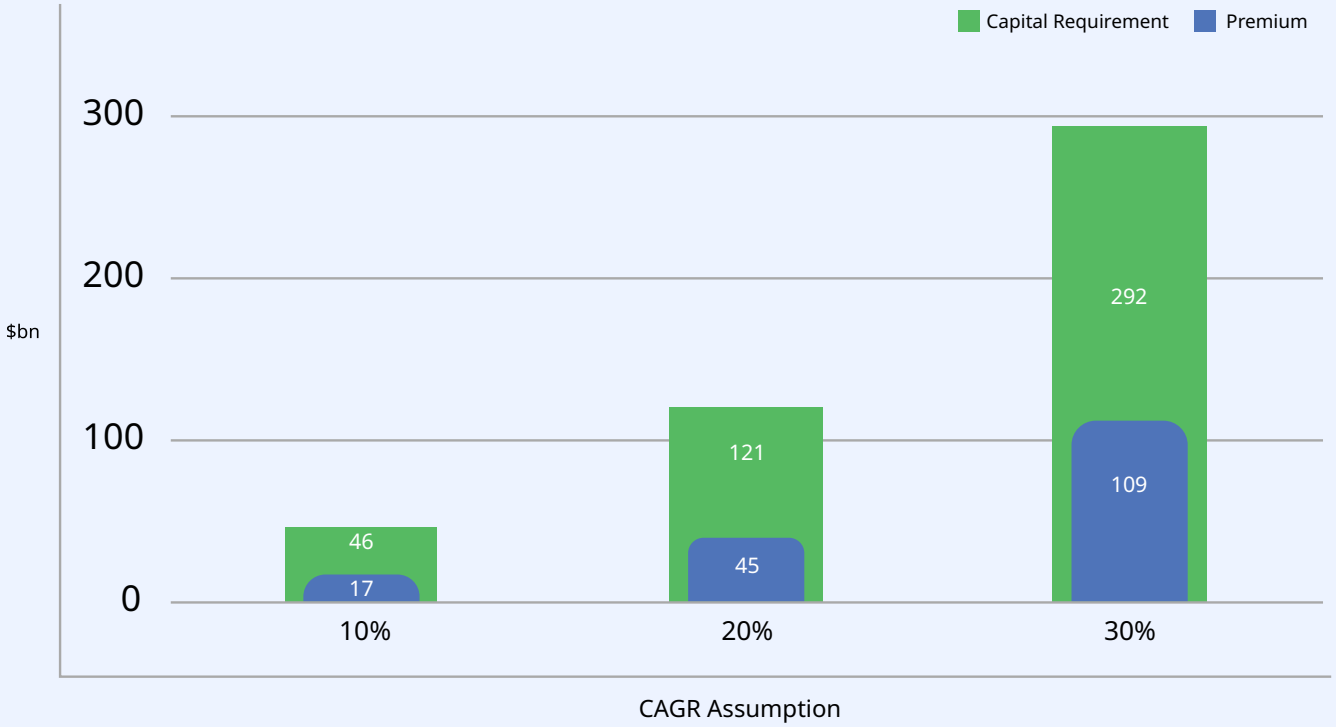
2. CyberCube's Exposure Databases comprise two primary elements: Economic Exposure Databases (EED) and Industry Exposure Databases (IED). This combination details information on insurable companies, their respective exposures, and a representation of the insured market. Note that the premium listed is for all US risks, whether that premium is written on a US or foreign balance sheet.

3. CyberCube's Portfolio Manager is the market's leading cyber portfolio modeling solution. Portfolio Manager ensures that customers can obtain robust, realistic, and validated views of potential financial loss.

At mid-range 10-year growth estimates of 20%, the following would be expected in 2034:

1. US standalone premium will stand at $45 bn (present value), a five-fold increase from today (see **Exhibit 1**). However, product innovation will be required to achieve real growth in exposures, rather than mainly rate increases, as seen in recent years. Given low penetration rates for coverage of cyber risk today, insurers and brokers need to achieve deeper penetration across organizations, offering larger limits and broader coverage with more clarity on terms and conditions.
2. Cyber will become a peak peril for P&C insurers, with potential losses exceeding those of the largest natural catastrophe event to date, Hurricane Katrina[4]. Regulators and ratings agencies will need to apply similar levels of rigor to how risk is being managed for cyber exposures as they currently apply to natural catastrophe risk.
3. Carriers will need $121 bn of capital to manage capital to 1-in-250 year loss, a 500% increase on current capital requirements. CyberCube proposes that diversifying capital sources will be required to support catastrophe exposures, predominantly from capital markets capacity in the form of insurance-linked instruments, and public-private partnerships with the federal government.

Exhibit 1: 10-year Premium and Capital Requirements Across a Range of US Insurance Market Growth Assumptions



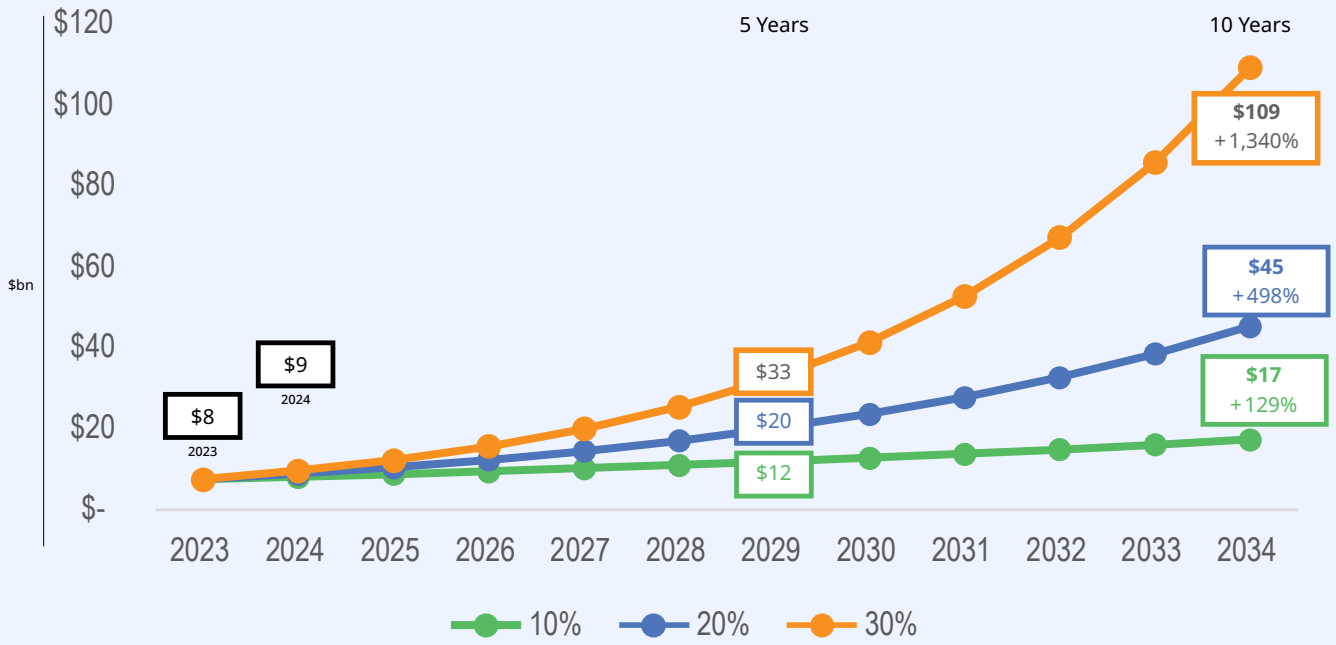
4. Hurricane Katrina, 2005 cost $102 bn Insurance Information Institute

5. CyberCube's Exposure Databases comprise two primary elements: the Economic Exposure Database (EED) and the Industry Exposure Database (IED). This combination details information on insurable companies, their respective exposures, and a representation of the insured market.

Substantial room for growth provided capital needs are met

Third-party commentators have broadly reached consensus on a CAGR of approximately 25% for the global cyber insurance market during the next two to 15 years[6]. CyberCube has taken a range of CAGR (see **Exhibit 2**) for US standalone cyber. Annual growth of 10% results in US standalone premium of $17 bn in today's dollars, 20% leads to $45 bn and 30% CAGR would reach $109 bn in 2034.

Exhibit 2: US Standalone Cyber Premium ($bn present value) Along Three Growth Trajectories



Given the uncertainty around the 10-year time horizon and recent volatility in growth for the US standalone market — which saw a 3% contraction in premiums written in 2022-23[7] — we believe this range provides a good basis for discussion on the potential of this market.

Using the mid-range projection, US standalone premium will reach $45 bn (present value), a five-fold increase on today. However, CyberCube's analysis of the purchasing patterns of US organizations highlights a marked shortfall in the number of organizations buying insurance today and the financial protection afforded by the limits on offer. Market growth cannot be achieved by predominantly relying on price increases, but by achieving real growth in exposures.

6. S&P, Munich Re, Gallagher Re, Jefferies https://content.naic.org/sites/default/files/inline-files/Final%202023%20Cyber%20Report.pdf, https://www.munichre.com/landingpage/en/cyber-insurance-risks-and-trends-2023.html, https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/future-of-cyber-re-insurance.pdf

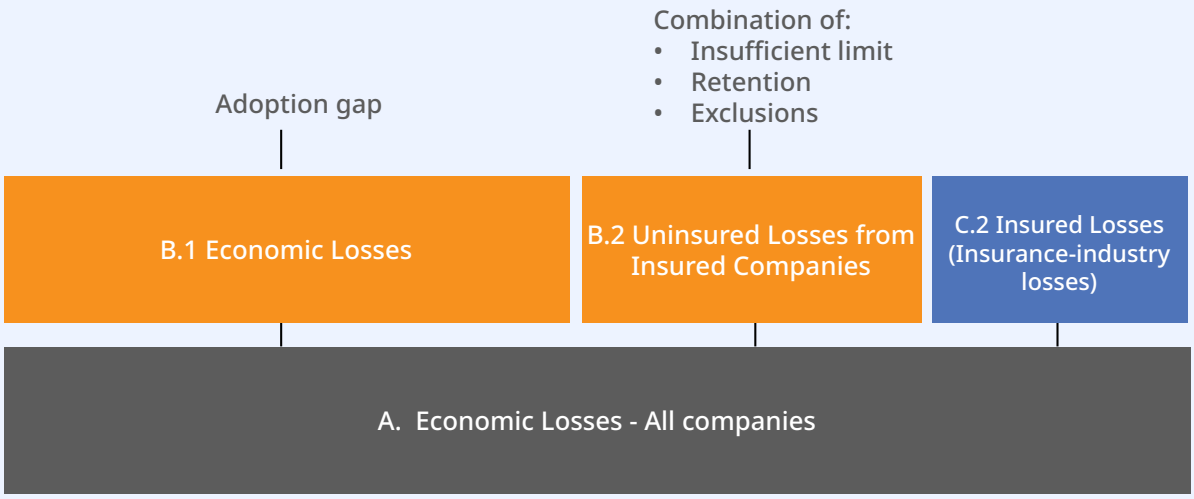
7. https://www.fitchratings.com/research/insurance/us-cyber-insurance-maintains-strong-profits-premium-growth-slows-16-04-2024

CyberCube's IED shows that almost three-quarters (72%) of large companies purchase some level of standalone cyber insurance in the US today. This drops to 43% for medium-sized companies, 12% for small, and just 3% take-up of standalone cyber for micro organizations. At the large organizations level, there is constraint on the ability of insurers to offer limits that afford meaningful financial protection in the event of a loss.

While the market can construct towers of several hundred million dollars of coverage for large organizations, CyberCube's *Broking Manager* tool[8] highlights many examples of underinsured companies. For example, one of the largest global IT companies has a 0.1% chance of losses $2.6 bn or greater, 0.5% chance of losses $1.5 bn or greater, and 1.0% chance of losses $1.1 bn or greater if they suffer a cyber incident. We see last year's slowdown in US premium growth as a temporary development for a market that has metabolized multiple years of major rate increases without real growth in insured exposure.

Several factors — such as low penetration of cyber insurance purchases among small businesses, insufficient limits for those businesses that do buy cyber insurance, and multi-decade secular trends toward greater digitization of the global economy — suggest that cyber insurance will continue to be a product with generationally robust demand growth (see **Exhibit 3**).

Exhibit 3: A Graphic View of the Shortfall in Companies Buying Insurance and the Amount of Cover They Purchase



- Based on CyberCube's Portfolio Manager catastrophe model – version 5.0
- Utilized CyberCube's 2023 Exposure Databases
- Based on 1-200 OEP

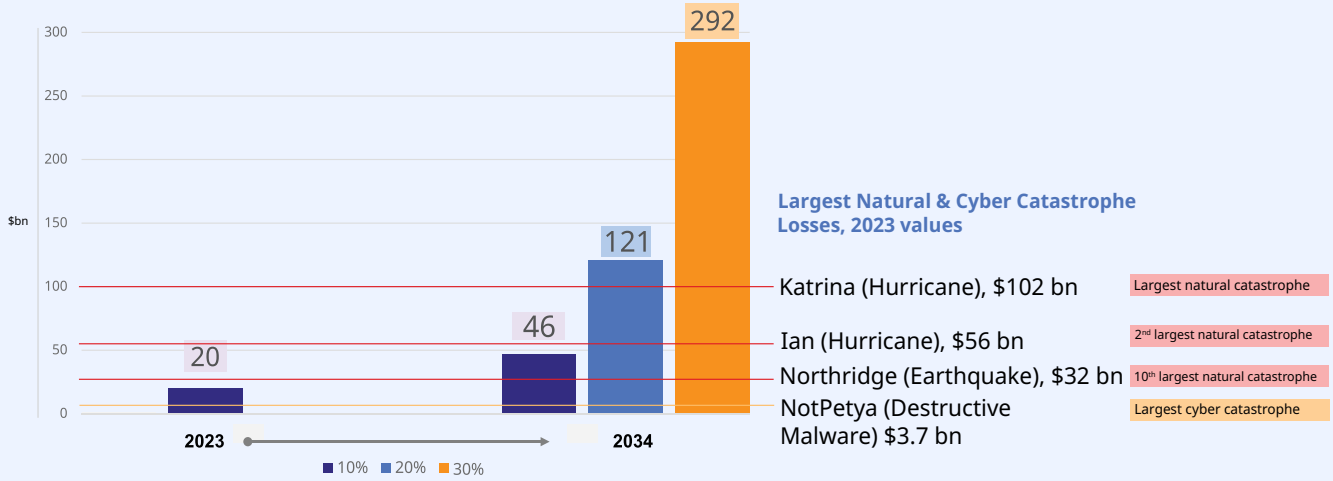
Insurers and brokers will need to accelerate current product innovation to achieve deeper penetration across organizations, offering larger limits and broader coverage with more clarity on terms and conditions. New markets may open up to diversify exposures away from peak cyber catastrophe scenarios. The growth of consumer and microbusiness cyber insurance markets, geographic and industry diversification, and new internet technology coverages will help build premium.

8. Broking Manager allows brokers to guide their clients through risk transfer strategies and prepare for the insurance placement process.

Peak peril to rival largest natural catastrophes

Cyber will become a peak peril for P&C insurers, with potential losses exceeding those of the largest natural catastrophe to date, Hurricane Katrina, at $102 bn (see **Exhibit 4**)[9].

Exhibit 4: Cyber Capital Compared to Major Aggregation Events



- Natural Catastrophe Sources: Insurance Information Institute, Facts + Statistics Global Catastrophes
- Worst Nat Cat years: Munich Re, Statista
- Cyber Catastrophe Sources: Claroty, PCS
- NotPetya Source: PCS, number shown in 2023 dollars.

Industry participants today employ a variety of methods for capital management (share of limits, internal models, multiple external models). In the absence of a clear market consensus approach, to estimate capital requirements in this analysis CyberCube has used tail metrics from Portfolio Manager, the market leading model by premium, and Insurance-Linked Securities (ILS) adoption.

"If a 20% CAGR is achieved by 2034, carriers will need to manage an estimated capital requirement of $121 bn — a 500% increase on current levels."

At the low end of the range (10% CAGR), cyber capital would exceed the 10th largest natural catastrophe (Northridge earthquake at $32 bn) and at the high end of the range, cyber capital could absorb 46% of the total global reinsurance capital available today[10]. The availability of capacity willing to assume catastrophic tail risk could be a constraint on market growth in light of this increased capital requirement. Traditional (re)insurance will certainly play an important role in providing such capacity, and we are encouraged to see the recent expansion of event cover offerings available to cedants.

The current cyber reinsurance market is tightly concentrated among the largest writers, so one implication is that the market will need broader participation from more reinsurers in order to sustainably distribute and share risk as the market expands. CyberCube proposes that additional sources of capital will be required to support such growth in catastrophe exposures. Two main sources for this capital could be capital markets capacity — in the form of insurance-linked instruments — and public-private partnerships, led by the federal government.

9. Hurricane Katrina, 2005 cost $102 bn Insurance Information Institute

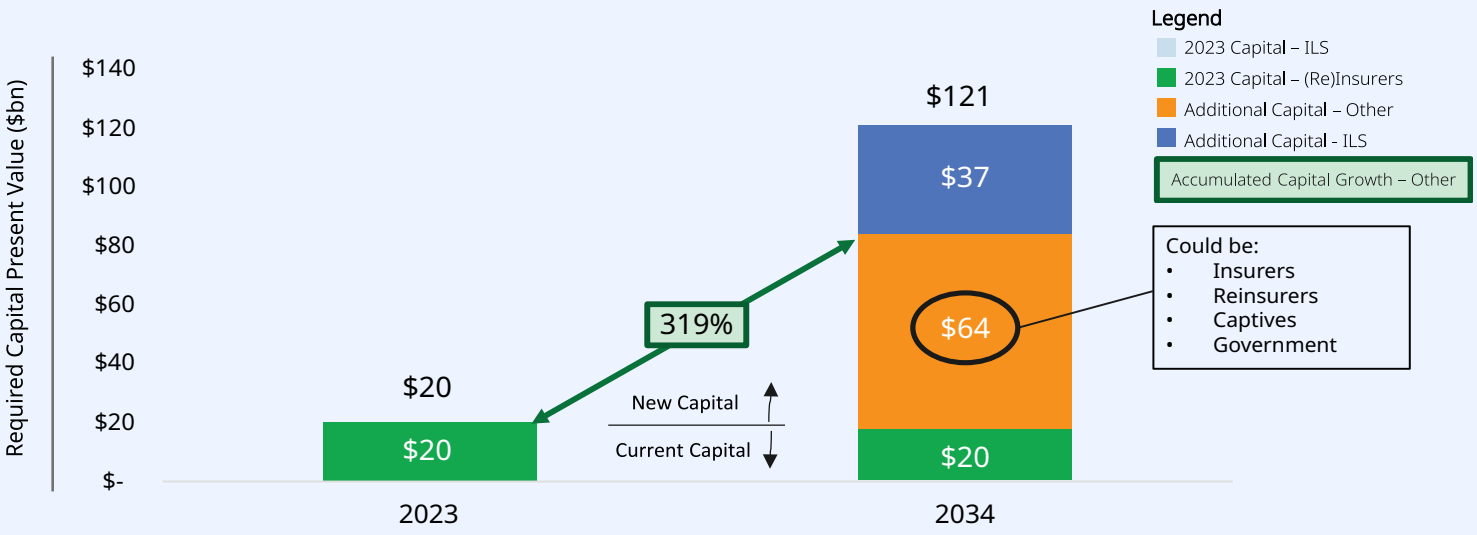
10. Aon, Reinsurance Market Dynamics 2024

Room to grow cyber ILS to US nat cat levels

The cyber ILS market is gaining some traction, with Artemis reporting almost $600 mn of issuance at June 2024[11]. In the final quarter of 2023, Axis Capital, Beazley, Chubb, and Swiss Re pioneered the introduction of 144A cyber catastrophe bonds, marking a significant evolution in the cyber (re)insurance arena. The launch of these four 144A bonds, alongside the first private cyber catastrophe bonds earlier in the year, illustrates the (re)insurance industry's forward-looking strategy to harness capital markets for mitigating and managing systemic cyber risk.

While this is a promising beginning, issuance still pales in comparison to the US Property ILS market. In 2023, CyberCube estimated approximately $37 bn of outstanding 144A bonds covering US Property peak exposures[12]. Even if the cyber ILS market size matches the Property ILS market size by 2034, (re)insurance capital will need to grow more than three-fold over the decade to meet required capital requirements. CyberCube modeled alternative capital growth for cyber across a range of scenarios, with the maximum reaching 100% of today's estimated $57 bn US property alternative capital market, including collateralized reinsurance, Industry Loss Warranties and other instruments[13].

Exhibit 5: Projected capital sources if 2034 cyber ILS matches 2023 Property ILS



Shown for 20% CAGR Market Growth

Data Notes:

- Contemplates only 144A (public) cat bonds, US Property Only
- 2023 ILS Source: Artemis as interpreted by CyberCube

Public-private partnerships will play a role for peak risk, as in nat cat

Closing the cyber protection gap is becoming increasingly important as our collective understanding of potential cyber catastrophes improves and the financial impact on individuals, businesses, and critical infrastructure becomes clearer. There are many examples of peak perils where private sector capital is unavailable at an appropriate quantity or price to meet society's

11. https://www.artemis.bm/dashboard/cat-bonds-ils-by-risk-or-peril/

12. Source: Artemis; analysis by CyberCube

13. 2023 global alternative capital = $101B (source: Aon Reinsurance Market Dynamics, Jan 2024). Assumes share deployed to U.S. is equal to the U.S.'s current share of global cyber premium (56%).

need for risk resilience; these include US terrorism, flood risk and peak hurricane zones. The Citizens Property Insurance Corp[14], a not-for-profit insurer, covers $650 bn of Florida homeowners exposure and the Florida Hurricane Catastrophe Fund, a state trust fund, has claims paying capacity of $17 bn[15]. The US federal government has also identified cyber risk as a major risk to the US economy - in 2023, the White House launched the National Cybersecurity Strategy as a coordinated effort to strengthen the resilience of the US economy to catastrophic cyber risk. In the mid-to-high range of cyber insurance growth projections, there is an increasing likelihood that the private sector will not be willing to assume all losses arising from the worst tail events. CyberCube expects the insurance sector innovations, outlined above, and public-private partnership initiatives will need to develop in tandem as the risk grows.

Capital efficiency will be a critical consideration

This report sought to begin the conversation about the great opportunity in front of the cyber (re)insurance market and to highlight a possible constraint — capital — that could inhibit the growth. As part of our research for this paper, we sought a range of feedback from market participants. The recurring theme in these discussions was the criticality of improving capital efficiency to meet the required capacity — and the challenge of articulating and quantifying how to do this with confidence. We believe there are additional levers that the insurance industry can and will explore to optimize capital efficiency that were not incorporated into this first perspective but are worthy of additional analysis.

These include, but are not limited to:

1. The impact of diversification across geographies.
2. New insurance offerings, such as personal cyber or cyber product liability, to broaden the base and diversify the peak cyber perils.
3. Further innovations in reinsurance structuring, such as event- and peril-specific towers and a greater usage of non-proportional coverage.
4. Continued refinements in cyber modeling approaches as we further test key assumptions and learn from future events.

Call to action to fulfill cyber insurance's growth potential

In all but the most pessimistic growth scenarios discussed in this paper, the cyber insurance market will need to make structural changes to support the growth of the cyber insurance market in a sustainable way. Some of these structural changes are starting to emerge and will require fuel to accelerate their growth — for example, penetration into the small business space and the emergence of the cyber ILS market. Some are still very much in their infancy and will require broader market collaboration to unlock, such as public-private partnerships that work for both sides.As the trusted partner in cyber risk analytics, CyberCube stands ready to deliver the data, analytics and expertise to empower cyber risk quantification and build resilience — unlocking the potential in this crucial area of risk transfer.

14. https://www.citizensfla.com/-/20220323-citizens-board-urges-cost-savings-as-market-conditions-remain-challenging#:~:text=Despite%20Citizens%27%20overall%20financial%20health,market%20continues%20to%20experience%20challenges.)

15. https://fhcf.sbafla.com/media/awmhd2tz/fhcf-may-2024-bonding-capacity-report.pdf

CyberCube

CyberCube is the leading provider of software-as-a-service cyber risk analytics to quantify cyber risk in financial terms. Driven by data and informed by insight, we harness the power of artificial intelligence to supplement our multi-disciplinary team. Our clients rely on our solutions to make informed decisions about managing and transferring cyber risks. We unpack complex cyber threats into clear, actionable strategies, translating cyber risk into financial impact on businesses, markets, and society as a whole.

CyberCube was established in 2015 within Symantec and now operates as a standalone company. Our models are built on an unparalleled ecosystem of data and validated by extensive model calibration, internally and externally. CyberCube is the leader in cyber risk quantification for the insurance industry, serving over 100 insurance institutions globally. The company's investors include Forgepoint Capital, HSCM Bermuda, and Morgan Stanley Tactical Value. For more information, please visit www.cybcube.com or email info@cybcube.com.

Lead Author

Alex Tenenbaum

Director of Services

Authors

Pascal Millaire

Chief Executive Officer

Rebecca Bole

Head of Industry Engagement

Jon Laux, FCAS

VP of Analytics

Content Editor

Yvette Essen

Head of Content, Communications & Creative

Design and Layout

Muhammad Ahmad

Graphic Designer