NEUBERGER BERMAN

CALLUM O'ROURKE, CFA
Vice President, Insurance-Linked Strategies

GEORGE CAUGHEY
Analyst, Insurance-Linked Strategies

Cyber Risk and ILS

Cyber risks are rapidly expanding, and with them the insurance industry designed to protect businesses and individuals from potential technology-related financial losses. In this paper, we provide an introduction to the cyber insurance market, explaining terms and coverage; we then explore the role of reinsurance in sharing cyber risks, and examine the relevance for investors in Insurance-Linked Securities.

Introduction

The cyber insurance industry exists to protect businesses and individuals from financial losses due to digital security breaches. According to PwC, 43% of 3,876 business and technology executives surveyed from the world's largest companies named cyber risk in their top 3 priorities for risk mitigation in 2024.[1] This awareness, often heightened through media coverage, translates into a growing demand for insurance coverage, increasingly seen as a core component of enterprise risk management.

In this white paper, we present a high-level overview of the cyber (re)insurance[2] market, including what is meant by cyber risk and what is typically covered. We then investigate how the industry currently quantifies, mitigates and models those risks. The role of traditional reinsurance is examined, along with the recent history and outlook of cyber risk transfer within Insurance-Linked Securities (ILS). Our paper is designed to give readers, especially ILS investors considering allocation to this peril, a clear picture of how the cyber (re) insurance market functions today.

Introducing Cyber Insurance Risks

Cyber risk refers to the potential for loss or damage resulting from a breach or failure of either an organization's or an individual's information technology systems. Attacks are typically inflicted by threat actors such as lone hackers, organized crime syndicates and state-sponsored groups, with a range of motivations; however, it is important to note that threats may also be non-malicious or accidental. Cyber threats can be categorized within the following five sub-peril groups:

- Data breaches
- Financial theft/business email compromise (BEC)
- Contagious malware
- Cloud outage
- Distributed Denial of Service (DDoS) attack

Cyber insurance coverage aims to protect individuals and organizations from financial losses arising from the above risks. The focus of this paper is on cyber insurance purchased by companies, but it is worth noting that personal insurance is a growing area of interest, with many insurance carriers offering protection via add-ons to homeowners' policies.[3] Insurance policies provide both first-party and third-party coverage. A non-exhaustive list of coverages is provided below.[4]

CYBER COVERAGE TYPES

First-Party		Third-Party	
Business Interruption (BI)	Loss of income due to an event that disrupts business operations	Data and/or Security Breach Liability	Costs associated with responding to a data breach (including notifications)
Data Recovery	Costs to recover lost data	Regulatory Defense	Costs associated with investigations or penalties from regulatory bodies
Cyber Extortion	Payments made in response to cyber extortion demands	Media Liability	Legal expenses resulting from insured's advertising or media activities
Funds Transfer Fraud	Financial loss following funds transfer fraud, fraudulent instruction, telephone fraud, etc.	Tech Errors & Omissions (E&O)	Errors and omissions of tech and software product/service providers

Source: CrowdStrike, August 12, 2022.

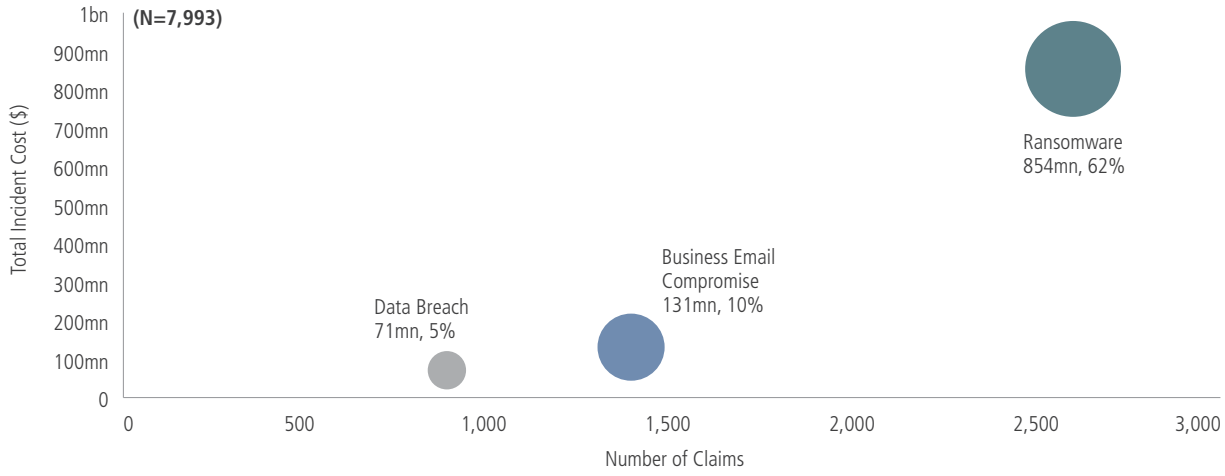
The terms and conditions of insurance policies for companies are based on features of the insured's organization, such as the industry in which it operates, revenue or size, type of data held (e.g., medical records), any implemented cybersecurity defenses and other factors.

[1] PwC, 2024 PwC, *2024 Global Digital Trust Insights.*
[2] (Re)insurance refers to both reinsurance and insurance.
[3] Metz, Jason, "Do You Need Personal Cyber Insurance," *Forbes* Advisor, June 10, 2023.
[4] Vaideeswaran, Narendran, "Cyber Insurance Explained," CrowdStrike, August 12, 2022.

NetDiligence's *Cyber Claims Study* report[5] provides statistics based on 9,028 global (predominantly from the U.S.) cyber insurance claims submitted by both small to medium enterprises (SMEs) and large companies[6] during the five-year period 2018 – 2022. Although SMEs submitted 98% of these claims, their estimated total incident cost (before any insurance payout), $1.6 billion, falls short of the $1.9 billion attributed to large companies. Ransomware,[7] Business Email Compromise (BEC) and Data Breach[8] are listed as the three main causes of insurance claims, with 62% of SME total incident cost over the period attributable to ransomware. While ransomware had the highest number of claims over the period, it is notable that ransomware activity levels are volatile. Although compiling a complete dataset on ransomware activity is challenging due to hesitancy by organizations to report attacks for fear of reputational damage,[9] another potential indicator of ransomware frequency is research by Chainalysis[10] on ransom payments facilitated by illicit crypto wallets monitored by the firm. In 2023 they estimate ransom payments through monitored systems (although not indicative of all ransom payments) hit $1.1 billion, a 98% increase from 2022 and surpassing the previous high of $939 million in 2021. This period of lower activity during 2022[11] is thought to be due to multiple possible causes, including the distraction caused by the Russia-Ukraine conflict to many of the ransomware groups operating from these territories.[12]

TOP THREE CAUSES OF LOSS – SMEs

Number of claims, aggregate incident cost, % of total incident cost



Source: NetDiligence, *Cyber Claims Study*, 2023.

When considering loss, it is important to distinguish between high-frequency, low-severity "attritional" losses and catastrophe losses. With respect to cyber, a catastrophe event[13] can be defined as:

1. A low frequency event that causes severe loss, injury or property damage to a large population of cyber risks; or
2. An event that starts with a disruption in either a service provider or a technology and unfolds by replicating this disruption whenever possible.

[5] NetDiligence, *Cyber Claims Study, 2023 Report.*
[6] SMEs defined as having less than $2bn annual revenue and large companies defined as having more than $2bn annual revenue.
[7] A type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files.
[8] Hacker as a cause of loss is assumed to be equivalent to Data Breach.
[9] Tokio Marine HCC, *2023 Cyber Report.*
[10] Chainalysis, "Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline," February 7, 2024.
[11] Cybernews, global ransomware attacks, as of February 2024.
[12] Tokio Marine HCC, *2023 Cyber Report.*
[13] Kovrr, *Cyber Catastrophes Explained*, September 2020.

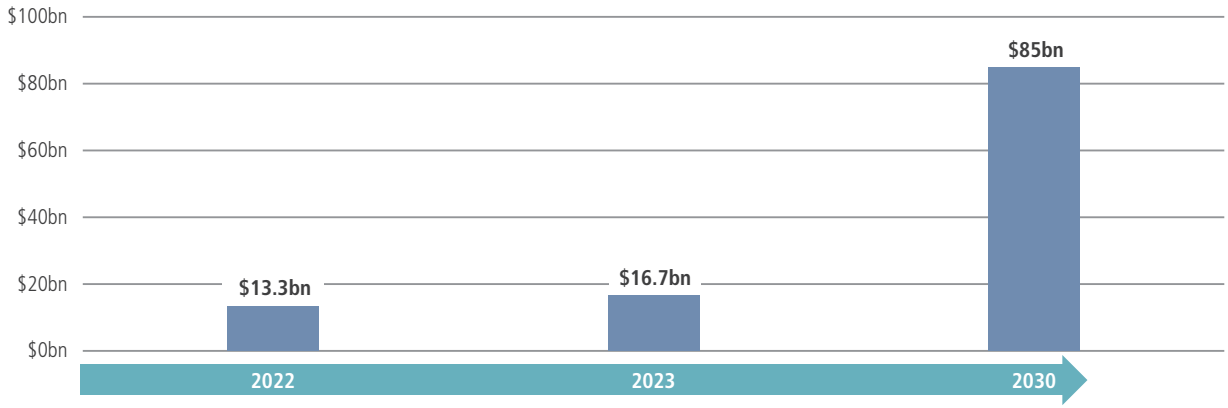
With respect to potential for catastrophe losses, most attention is given to a prolonged cloud outage event or a virulent strain of malware (including ransomware) targeting vulnerabilities in a widely used piece of software, causing widespread disruption to both business and operations.[14]

As for the future, artificial intelligence (AI) is an example of the evolving and dynamic nature of the cyber risk landscape. Although there are many benefits to integrating AI into cybersecurity methods,[15] AI technology is increasingly mentioned as a potential source of attack, allowing threat actors to execute more intelligent and adaptive threats that can learn from past attempts.[16]

Cyber (Re)Insurance Market Dynamics

The rapidly growing demand for cyber insurance coverage is reflected in the estimated 25% growth of global Gross Written Premium (GWP) between 2022 and 2023.[17] This momentum is expected to be sustained, with GWP forecasted to reach $85 billion by 2030, exhibiting a compound annual growth rate of 26.1%.[18]

GLOBAL GROSS WRITTEN PREMIUM FORECAST

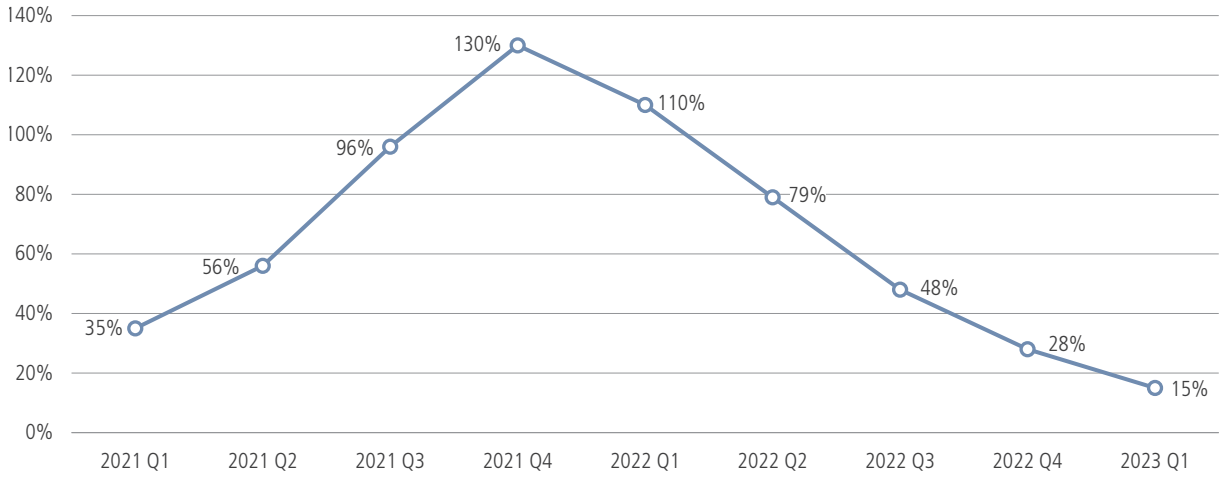


Source: *Fortune* Business Insights, April 2023.

A higher perceived level of risk and increased demand for protection following the wave of ransomware attacks in 2019[19] enabled insurance providers to benefit from favorable market conditions from 2020 – 2022, with Marsh's insurance market rate index showing that there were quarterly increases in average rate[20] for cyber policies underwritten in the U.S. over the period. We believe the subsequent decrease in ransomware activity in 2022[21] was likely a contributing factor to the near flat rate change across U.S. renewal policies in 2023.[22]

[14] Gallagher Re, The Risk of a Cyber Catastrophe, 2023.
[15] Deloitte LLP, *Smart cyber: How AI can help manage cyber risk*.
[16] Gregory, Jennifer, "AI Security Threats: The Real Risk Behind Science Fiction Scenarios," *Security Intelligence*, May 15, 2021.
[17] *Fortune* Business Insights, *Cyber Insurance Market Size, Share & COVID-19 Impact Analysis*, April 2023.
[18] Ibid.
[19] Tokio Marine HCC, *2023 Cyber Report*.
[20] Rate is defined as premium price per unit of insurance coverage.
[21] Tokio Marine HCC, *2023 Cyber Report.*
[22] Marsh Global Insurance Market Index, 2023.

U.S. CYBER RATE CHANGE (2021 – 2023)



Source: Marsh U.S. Insurance Market Index, 2023.

Reinsurance capacity has been crucial in supporting a sustainable cyber insurance market, and primary insurers currently cede approximately 45% of direct cyber GWP to reinsurers to reduce their potential liability.[23] For the cyber insurance market to grow to its forecasted 2030 size, the reinsurance market will also need to grow significantly to meet this demand. Regarding preferred reinsurance structures, in the initial stages of the cyber reinsurance market, quota share (QS) structures,[24] where reinsurers share the risk and reward with the ceding insurer(s), were typically favored. QS structures continue to be the most widely adopted to date, but despite their relative dominance, the number of event-based excess-of-loss reinsurance programs is increasing,[25] likely due to insurers looking for more efficient means to protect themselves against catastrophe events.

Mitigating and Quantifying Cyber Risks

Although price changes for insurance coverage have been a major component of the cyber insurance market's response to losses, since 2021 the underwriting process has become a focus, with many insurers adopting more stringent underwriting criteria and sophisticated risk assessment tools.[26]

Many insurers now proactively assist insureds to implement strategies to minimize system vulnerabilities—and insureds demonstrating strong "cyber hygiene" are typically rewarded with premium discounts.[27] In addition, insurers can use monitoring tools to identify vulnerabilities in real time and notify insureds during policy periods.[28] If insureds do not respond adequately to the vulnerability notification (e.g., by implementing a patch), this can affect their coverage. A focus on exclusions, particularly for general infrastructure and war events, coupled with higher deductibles and the wider usage of sub-limits, have also reduced insurers' exposure to surprise losses and increased the quality of portfolios.[29]

In addition to the underwriting approaches discussed above, (re)insurers are also utilizing third-party vendor models to quantify cyber risk, especially with respect to catastrophe. One of the challenges of modeling cyber risk is a limited historical dataset, making it difficult to produce statistically robust predictions regarding "high severity, low frequency" events. Furthermore, cyber risk is characterized by a significant number of "unknown unknowns" due to a triumvirate of rapid technological advances, adaptive threat actors and the general unpredictability of human behavior. Earlier models were very "black box", with little transparency into

[23] *Global (Re)Insurance, "Global cyber premiums could exceed $50bn by 2030 – Howden,"* July 6, 2023.
[24] Lockton Re, *Reinsurance, Unlocking Potential – Why Now Is the Time Cyber ILS Has the Momentum to Succeed*, February 2023.
[25] Guy Carpenter & Co., *Through the Looking Glass: Interrogating the key numbers behind today's cyber market*, 2023.
[26] Gallagher Re, *CY – FI, The Future of Cyber (Re)insurance*, 2022.
[27] Kost, Edward, "8 Tips for Lowering Your Cyber Insurance Premium in 2024," UpGuard, January 18, 2024.
[28] Gallagher Re, *CY – FI, The Future of Cyber (Re)insurance*, 2022.
[29] Lockton Re, *Reinsurance, Unlocking Potential – Why Now Is the Time Cyber ILS Has the Momentum to Succeed,* February 2023

methodology and how numbers were derived.[30] Naturally, demand for more sophisticated models, underpinned by logical assumptions to capture the causal relationships of an increasingly technologically reliant and interconnected world, has increased with the growth of the cyber insurance market.

The challenge of modeling a "high severity, low frequency" peril like cyber is the same in the natural-catastrophe space and, consequently, the broad modeling framework adopted by vendors can be split into similar components: hazard, vulnerability and financial. The hazard component generates an event set using simulation techniques, with the aim of capturing the range of cyber incidents that could happen outside the observed historical record; each event corresponding to a hypothetical threat or attack of a certain severity, such as a 48-hour cloud service outage across a set of datacenters. Determination of how often each event is expected to occur (the frequency) varies, but expert judgment is needed, since a significant human element is inherent within cyber compared with natural perils.[31] Next, the vulnerability component dictates how each policyholder in an insurance portfolio is economically impacted by a given event and is typically a function of company-specific information such as annual revenue, industry, technology systems and geography. Finally, the financial component determines the cost incurred by the insurer after application of all terms and conditions across all impacted policies.

Today, multiple vendors offer views of cyber risk with similar probabilistic outputs from natural-catastrophe models, allowing the calculation of familiar metrics like expected loss[32] the *lingua franca* of modeled risk within ILS. Three of these modelers are considered leaders: CyberCube, a cyber specialist founded in 2015, GuideWire, incorporated in 2001, with a model known as Cyence and Moody's Risk Management Solutions (RMS), a market leader in the natural catastrophe modeling space.

Despite cyber modeling being in its relative infancy, it is still notable how much each vendor's view of risk diverges. Data from a recent Guy Carpenter[33] report shows that cyber industry losses globally at the 50- and 200-year return period across various geographies are noticeably higher in CyberCube compared with RMS; for instance, the 50-year return period loss for U.S. losses using CyberCube is four times that of Moody's RMS at roughly $17 billion.

MODELED LOSSES AT 50- AND 200-YEAR RETURN PERIOD (USD)

Return Period	CyberCube V4	Cyence M5	Moody's RMS V6
Global			
50	24.4 billion	10.0 billion	5.5 billion
200	33.4 billion	25.8 billion	15.6 billion
U.S.			
50	16.9 billion	6.6 billion	3.5 billion
200	23.4 billion	17.6 billion	10.0 billion
International			
50	8.3 billion	3.5 billion	2.4 billion
200	10.7 billion	9.5 billion	6.1 billion

Source: Guy Carpenter & Co., June 2023.

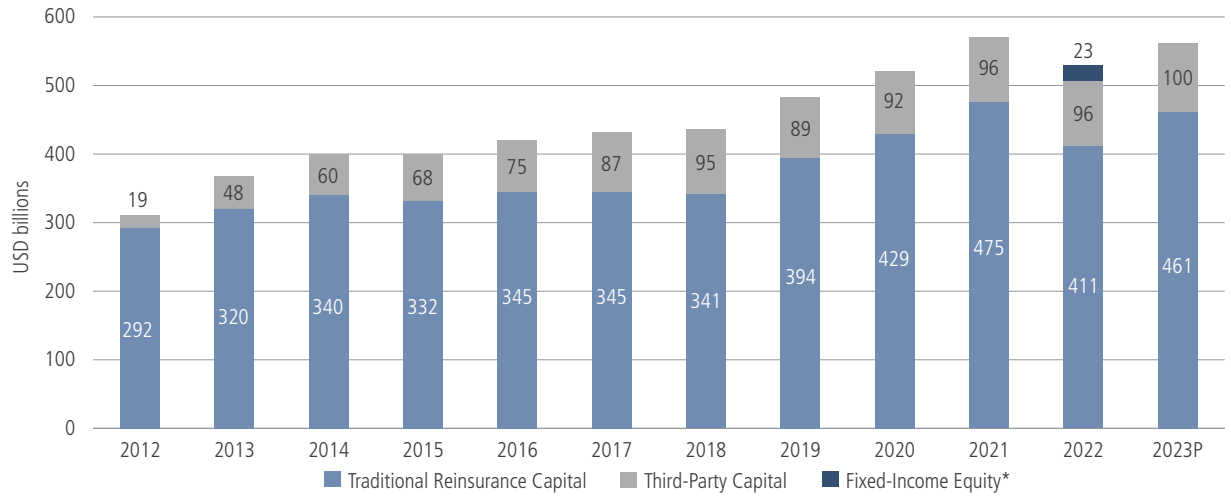
Although cyber modeling is inherently uncertain, this is not unfamiliar territory for catastrophe model practitioners and precisely why models exist. As models continue to improve with more data and lessons from observed events, confidence in both the models and intuition should increase. With respect to the differing views of risk across models, a multimodel approach is most useful in understanding the potential range of risk in an underlying portfolio of exposures.

[30] Gallagher Re, *Evaluating Cyber Models*, 2022.
[31] Lockton Re, *Reinsurance, Unlocking Potential – Why Now Is the Time Cyber ILS Has the Momentum to Succeed*, February 2023.
[32] Expected loss is measured as the model derived loss frequency multiplied by loss severity summed for all simulated events.
[33] Guy Carpenter & Co., *Through the Looking Glass: Interrogating the key numbers behind today's cyber market*, 2023.

History of Cyber ILS

Today, ILS are well established as a risk-transfer mechanism for (re)insurance markets, providing an estimated 18%[34] of the total capital in the global reinsurance market in 2023.

ESTIMATED CONTRIBUTION TO GLOBAL REINSURANCE CAPITAL



*Fixed-Income Equity is the amount that AM Best anticipates will be recovered as bonds mature over time.
Source: Artemis, as of December 29, 2023.

The perils covered by most ILS transactions are natural, but the mechanism has been used for transactions exposed to other risks such as aviation, terrorism, longevity and mortality. Since 2015, ILS have been considered a potential provider of additional capacity into the cyber insurance marketplace.[35] However, 2023 marked a new milestone when AXIS issued the first ever public 144a[36] cyber catastrophe bond, providing $75 million of coverage. The bond is an indemnity structure, which means that its payout is determined by actual insured losses incurred by AXIS due to a covered cyber event.[37] Since the successful placement of this transaction, there have been an additional three issuances, bringing the total to $415 million in notional limit. Of these three, two were also indemnity, but the Swiss Re transaction is based on an industry-loss index—meaning that the payout is determined by cyber insurance losses to the whole industry as reported by a third-party loss reporting agent.

Regarding risk, from each issuance's expected loss we can deduce that these bonds are relatively risk-remote, with modeled expected losses in the 1 – 2% range (which approximately corresponds to coverage between a one-in-100-year and one-in-50-year cyber event). Further, the Swiss Re industry-index bond would trigger should reported U.S. cyber insurance industry losses from a single event exceed $9 billion,[38] which is approximately 30 times greater than the largest known cyber insurance industry loss: NotPetya, which was a 2017 ransomware event that caused an estimated $300 million loss to cyber policies out of a total insurance industry loss of approximately $3 billion.[39] Risk-adjusted pricing is relatively strong, with the weighted-average multiple[40] of these issuances at 7.6, and no single multiple falling below the weighted-average multiple of 4.5 across all 144a catastrophe bond issuances for 4Q.

[34] Evans, Steve, "*ILS capital outpaced AM Best/Guy Carpenter forecast to hit $100bn in 2023*," Artemis, December 29, 2023.
[35] Lockton Re, *Reinsurance, Unlocking Potential – Why Now Is the Time Cyber ILS Has the Momentum to Succeed*, February 2023.
[36] Rule 144A is a U.S. legal provision that amends restrictions placed on trades of privately placed securities; it loosens restrictions set forth by Rule 144 under Section 5 of the Securities Act of 1933.
[37] Evans, Steve, "AXIS sponsoring the first 144a cyber cat bond, $75m Long Walk Re," Artemis, October 18, 2023.
[38] Artemis, "Matterhorn Re Ltd. (Series 2023-1)," Artemis Catastrophe Bond and Insurance-linked Securities Deal Directory.
[39] Gallin, Luke, "Silent cyber drives Petya loss to $2.7 billion," Reinsurance News, May 23, 2018.
[40] Multiple is the ratio of a bond's spread to its expected loss, effectively representing the bond's risk-adjusted earnings ratio.

UNIVERSE OF CYBER 144A TRANSACTIONS

Issue Name	Sponsor	Size	Expected Loss	Spread[41]	Multiple	Issuance	Maturity
Matterhorn 2023-1	Swiss Re	$50,000,000	1.72%	12.00%	7.0	Dec 2023	Aug 2026
East Lane Re 2024-1	Chubb	$150,000,000	1.39%	9.25%	6.7	Dec 2023	Mar 2026
PoleStar Re 2024-1	Beazley	$140,000,000	1.26%	13.00%	10.3	Dec 2023	Jul 2026
Long Walk Re 2024-1	AXIS	$75,000,000	1.97%	9.75%	5.0	Nov 2023	Jan 2026

Trigger Type: Industry-Index Indemnity

Source: Artemis, data as of February 14, 2024.

Outlook for ILS in Cyber Reinsurance

As mentioned, since the cyber insurance market size is projected to increase, with a compound annual growth rate of 26.1% in GWP until 2030, we believe ILS will likely play a crucial role in providing additional capital to support this growth. Consequently, we anticipate that the momentum of recent catastrophe bond issuances will extend into 2024 and beyond.

Investors can draw confidence from recent rate stabilization, signaling a growing maturity in underwriting practices, where insurance carriers are confident premiums being paid are commensurate with the risk being underwritten (rate adequacy). Further, the noted ability of insurance companies to deploy risk mitigation strategies in real time by proactively monitoring vulnerabilities and the response of their policyholders should bring further comfort to risk-takers.

The successful placement of catastrophe bond issuances at the end of 2023 suggests that a certain consensus was reached by the ILS investor community in attempts to address historical challenges in cyber-ILS placement, such as event definition and modeling. In addition, from a risk-adjusted perspective, the relatively high multiples available should also be reassuring to investors, since any concerns around cyber models and corresponding modeled expected loss numbers must be compensated fairly.

One significant challenge where there is still work to do is in cyber event definition, given the difficulty of defining a single event for a peril that is amorphous in nature, to ensure that similar but unique events are not incorrectly aggregated. In addition, how the date of loss and reporting window are determined is important for coverage providers, since for any given cyber event, claims may be submitted over an extended timeframe; for some events there is often a significant delay between when the incident occurs and when a policyholder detects it. Recent 144a cyber catastrophe bonds addressed these challenges by limiting the number of days during which losses can be attributed to a single event, with input from the ILS investor community.

Another definitional challenge is ensuring the effectiveness of exclusions. Nevertheless, efforts made by industry bodies such as the Lloyd's Market Association (LMA) to standardize exclusionary language, particularly for systemic events arising from war, critical infrastructure failure and state-on-state operations[42] contribute to a clearer understanding of the risks covered in ILS transactions. As more issuances come to market, ILS investors should have an opportunity to contribute to further refinement of event definitions.

As the ILS market continues to grow, the addition of new perils and regions that increase the opportunity set available for portfolio construction is beneficial. Cyber has an inherent diversification benefit if added to existing ILS portfolios since it is uncorrelated with the occurrence of natural catastrophe events.[43] However, it is important to touch on the potential correlation a cyber catastrophe could have with systemic risks in other financial markets such as equities and fixed income. To have a material impact on the global financial system, such an event would need to be sustained over a significant period, severely affecting a wide swathe of industries and geographies. Since core components of internet infrastructure are segmented, not built on uniform technology and with regional differences in terms of workflow, the likelihood of such a global contagion event is extremely low.[44] Furthermore, factors like insurers' focus on exclusions and

[41] Spread is defined as the fixed interest payment expressed as a percentage of the par value of the bond.
[42] Lockton Re, Reinsurance, *Unlocking Potential – Why Now Is the Time Cyber ILS Has the Momentum to Succeed*, February 2023.
[43] Braun, Alexander, et. al., "Cyber insurance-linked securities," Cambridge University Press, June 8, 2023.
[44] Lockton Re, *Reinsurance, Unlocking Potential – Why Now Is the Time Cyber ILS Has the Momentum to Succeed*, February 2023.

proactive monitoring of vulnerabilities lower the potential for a cyber catastrophe, further diluting correlation with other financial markets. Therefore, we believe the axiom that there is a diversification benefit to a multi-asset portfolio through allocation to ILS holds, even with the inclusion of cyber.

Conclusion

In our view, cyber (re)insurance is essential for financial protection against information technology threats and is set to become even more embedded in risk management practices. ILS have already supported market growth, and 2023 was a significant milestone, with the first-ever public 144a catastrophe bonds covering cyber perils providing a total of $415 million of capacity.

We believe that cyber as a proportion of total ILS issuance will continue to grow, and although there are complexities unique to the peril, our understanding and capabilities in quantifying this risk have improved rapidly over a short time and this should continue. In addition, steps taken by insurers, such as proactive risk mitigation and a focus on clearly defined policy language to improve the quality of their portfolios, will ensure that this growth is sustainable.

We take the view that as long as strong risk-adjusted pricing continues and accounts adequately for modeling uncertainty, cyber can be considered a valid diversifying option for allocation to ILS portfolios.

NEUBERGER | BERMAN

Neuberger Berman
1290 Avenue of the Americas
New York, NY 10104-0001

www.nb.com