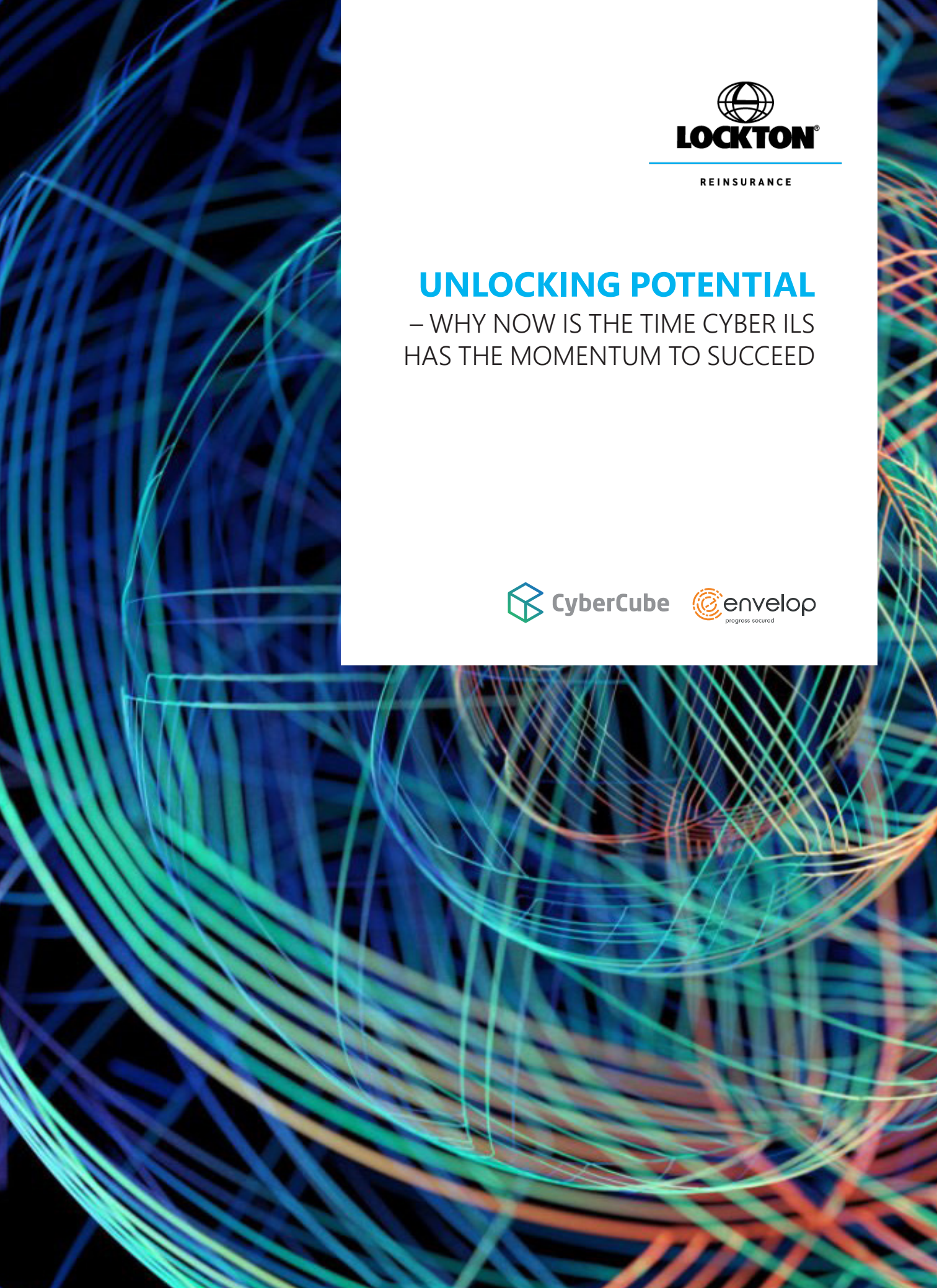


LOCKTON®

REINSURANCE

UNLOCKING POTENTIAL

– WHY NOW IS THE TIME CYBER ILS HAS THE MOMENTUM TO SUCCEED

CyberCube

envelop

progress secured

HELPING BUSINESS UNDERSTAND, MITIGATE AND CAPITALISE ON RISK.

Lockton Re's reports, market commentary and insights focus on key topics, occurrences or changes in the (re)insurance and broking market place which impact our clients and partners. In order to help guide relevance for the reader we categorise this content in four areas – Exposures, Perils, Risk Transfer and Placement. In this report we have collaborated with CyberCube and Envelop to create a broader perspective. Together we are very well placed to comment on this area of increased interest. Lockton Re looks forward to working on behalf of our clients to deliver new insights and innovative products designed to address the multifaceted cyber risk environment.

About Lockton Re (locktonre.com)

Lockton Re, the global reinsurance business of Lockton Companies, helps businesses understand, mitigate, and capitalise on risk. With over 300 colleagues in 15 locations globally, the business is continuing to grow, pushing the reinsurance industry forward with smarter solutions that leverage new technologies—delivered by people empowered to do what's right for clients.

About Envelop Risk (enveloprisk.com)

Envelop Risk is a global specialty cyber underwriting firm based in London (UK) and Bermuda. The firm began underwriting cyber risk in late 2018 and has established itself as a leading cyber reinsurer globally, with over US$600m in GWP underwritten to date. Envelop's mission is to become the leading global capital allocator for cyber-related risk by combining superior capital management, underwriting, structuring, and data-driven proprietary modelling.

Envelop's advanced cyber modelling tools include threat intelligence, cyber posture analytics, global economic and financial data, and comprehensive global claims history. The firm is backed by Softbank Vision Fund 2, MS Reinsurance, Alpha Intelligence Capital, Integra Partners, and Chimera Abu Dhabi.

About CyberCube (cybcube.com)

CyberCube delivers the world's leading cyber risk analytics for the insurance industry. With best-in-class data access and advanced multi-disciplinary analytics, the company's cloud-based platform helps insurance organisations quantify cyber risk to facilitate placing insurance, underwriting cyber risk and managing cyber risk aggregation. CyberCube's enterprise intelligence layer provides insights on millions of companies globally and includes modeling on thousands of points of technology failure.

The CyberCube platform was established in 2015 within Symantec and now operates as a standalone company exclusively focused on the insurance industry, with access to an unparalleled ecosystem of data partners. It is backed by Morgan Stanley Tactical Value, Forgepoint Capital, HSCM Bermuda, MTech Capital, individuals from Stone Point Capital and Scott G. Stephenson. For more information, please visit our website or email info@cybcube.com.

• Exposure • **Peril** • **Risk Transfer** • Placement

Executive Summary

Insurance-Linked Securities (ILS) have played a key role in allowing catastrophe risk to be transferred from the commercial insurance market to investors, providing much needed additional (re)insurance capacity. There has been talk for years about the potential of cyber ILS to transform the cyber insurance market. The conditions of the market today are at a point where this potential can be fulfilled. There is:

- **improved understanding of the peril**
- **convergence on trigger type**
- **better data to assess cyber catastrophe risk**
- **a growing consensus around model usage**

All these factors enable cyber ILS to emerge as a meaningful provider of much needed additional capital to support continued growth of the cyber insurance market.

Catastrophe risk driving innovation

In August 1992, Hurricane Andrew devastated many parts of Florida and the southern United States. It became notorious for the terrible property destruction and loss of life. But the far-reaching consequences for the (re)insurance industry lasted long after the rebuilding was complete. It became an inflection point for (re)insurers and regulators – more than a dozen insurers were declared insolvent due to the scale of the losses, with insured claims of over US$53 billion[1] in today's dollars.

There was a critical development because of the storm: the emergence of the ILS market. This enabled insurance risk to be transferred to investors in the form of a tradeable security. ILS focused on providing (re)insurance capacity for extreme natural catastrophe events and trading in niche areas of property catastrophe (re)insurance until another dramatic milestone: the significant cumulative losses caused by hurricanes Katrina, Wilma, and Rita in 2005. Insured losses alone were over US$98.5 billion[2] in today's dollars. Capital markets were able to address the subsequent capacity shortage and provided a critical injection of over US$8 billion of catastrophe bonds in 2007. Since then, as illustrated in Figure 1 the ILS market has grown exponentially and with a cumulative cat bond issuance of US$120 billion[3] from 2007 to today.

[1]https://news.ambest.com/articlecontent.aspx?refnum=321994&altsrc=2 adjusted for inflation based on CPI index
[2]https://www.swissre.com/dam/jcr:a835acae-c433-4bdb-96d1-a154dd6b88ea/hurrican-katrina-brochure-usletter-web.pdf adjusted for inflation based on CPI index
[3]https://www.actuary.org/sites/default/files/2022-06/ILS_20220614.pdf

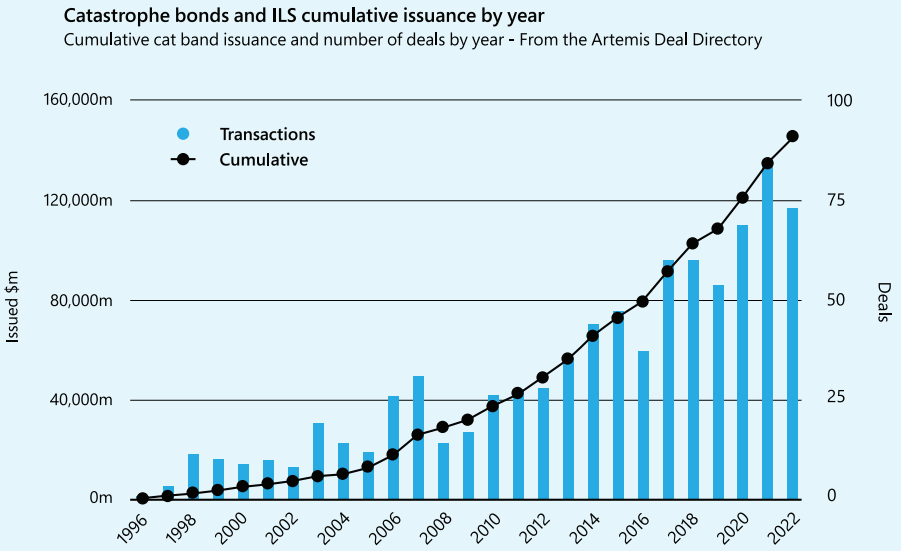


Figure 1. The dramatic growth of the ILS market in the last 25 years
Source: www.Artemis.bm Deal Directory

Perils covered in ILS transactions have evolved significantly as shown in Figure 2, from the peak natural catastrophes of hurricane and earthquake to broader natural perils including wildfire, winter storm, severe thunderstorms, and flood as well as non-natural perils including mortgages, mortality, and longevity. The potential for cyber risk to be used as the basis for ILS investments was identified as early as 2015 in the insurance trade press, and the unfulfilled potential has been the topic of much debate since then. In this paper, the case is made that the time and the market is right for ILS investors to enter cyber insurance in a meaningful way. One by one, the issues which have held back the material development of the cyber ILS market are being addressed. As the cyber insurance market has matured, so the concerns of both (re) insurers and investors recede.

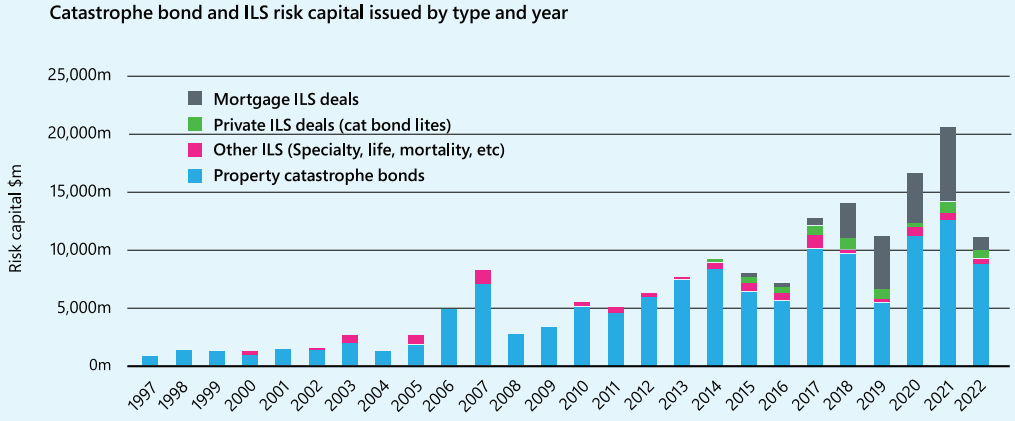


Figure 2. The range of perils for the ILS investors has increased materially in the last few years
Source: www.Artemis.bm Deal Directory

Straining at the Leash

The cyber insurance market has evolved significantly in the last few years. The understanding of the fast-changing nature of the peril has increased and there is much more dedicated cyber security expertise now embedded within the insurance industry. This has enabled a more sophisticated assessment of the threats, more effective communication with technical buyers, and an ability to provide growing level of comfort within senior management at carriers.

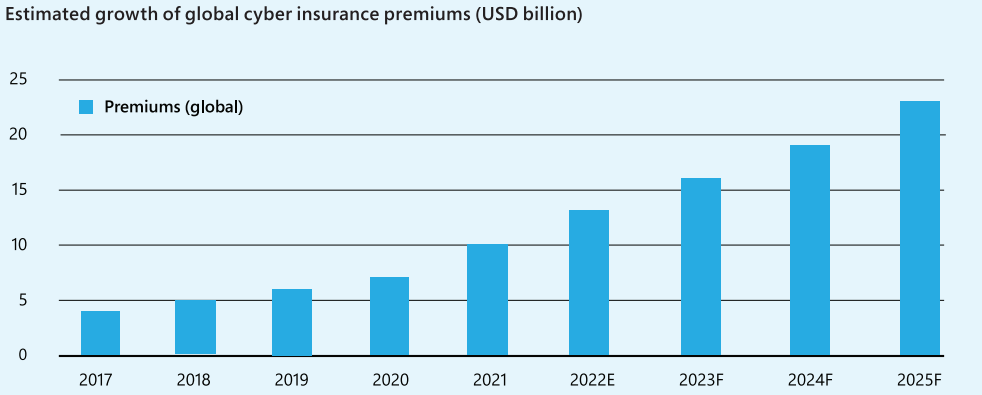


Figure 3. The dramatic growth of the cyber insurance market is expected to continue for years to come
Note: E =estimates, F=forecasts. Swiss Re estimates/forecasts comprise standalone and packaged cyber policies
Source: Swiss Re Institute

> "Cyber insurance is considered a core specialty insurance line by many enterprises, and no longer a luxury purchase, with demand continuing to increase."

This growth is expected to continue for years to come, as shown in Figure 3. The multi-faceted risk landscape is better understood, as is the role insurance plays, alongside technical and procedural controls to protect companies and build resilience against a myriad of risks, ranging from rogue employees, criminal hackers, and politically-motivated activists. Rates have increased in response to rising claims, so the value of the insurance has been demonstrated over many years. Entire new segments are beginning to show promise such as cyber products for personal lines. Longer-term, some other lines of business may be (partially) subsumed into cyber – for example auto insurance will need to consider the cyber threat to autonomous driving systems. Additionally, there are vast greenfield opportunities for potential buyers in new territories as well.

The continued growth of the market must overcome concerns in two areas for its continued expansion. Firstly, attracting additional financial capacity to support the solvency requirements as premium grows; and secondly, building confidence

around the potential downside, especially as it relates to systemic risk. These issues are interconnected and by addressing these challenges, the massive untapped potential of the market can be unleashed. There remains a huge "protection gap" between the current levels of cyber insurance purchased, and the total estimated economic consequences of cyber-attacks. These cybercrime costs are on track to increase to over US$10 trillion[4] by 2025.

Consensus on trigger type

Early natural catastrophe ILS transactions utilising parametric triggers had the benefit of clarity in their purpose and scope. If a named storm hit a specific geographic area at a certain speed, a pay-out was made. There has been much debate in cyber insurance circles around how to define an analogous event which is a discretely identified insured peril and can be measured appropriately. One challenge has been the mismatch in expectations between potential protection buyers (sponsors) seeking all-peril cyber coverage ILS structures on one side, and investors on the other side more interested in transactions which have only very specific, clearly defined cyber perils included. The peril being covered needs a common understanding of its nature and the event definition is key.

> "One misconception by some ILS investors is that all cyber risk is global."

Interconnected technology operates without interruption in a borderless world. In this scenario, unlike specified named perils, in theory all cyber risk could cascade across all companies around the world. The reality is different. Although there clearly are some elements of connectivity between regions, there is significant segmentation built into the large global internet infrastructure providers. Additionally, there are inherent cultural variations and adaptations in how companies build and rely on different key technologies, so there is a complex patchwork of different technologies across industries and geographies, leading to a much lower risk of a single vulnerability spreading globally. One way to limit this risk within the ILS context is to impose geographic conditions on a transaction. Depending on the portfolio, this could be a valuable way to address these concerns.

In the world of property cat reinsurance, trigger types are often broken down into three main categories: ultimate net loss (UNL), parametric and insured industry-loss (index). All three are traded as part of excess of loss reinsurance structures, with ILS investors able to assume this risk via various means. Additionally, some (re)insurance companies offer specialist fronting services, which can provide valuable non-recourse leverage to the end consumers of risk. Other third parties specialise in the provision of licensed transformer vehicles able to write reinsurance and package it into securities.

These risk transfer mechanisms, and the associated market infrastructure can be harnessed and used for cyber ILS, though certain nuances of cyber are acknowledged. The selection of trigger type will vary based on the particulars of a transaction, but there is an emerging consensus that each of these can serve the needs of the cyber insurance market in different contexts. The concept of parametric triggers translates naturally from property cat into the world of cyber reinsurance. The mechanics and rationale are unaltered: the need for an independent, competent calculation agent to determine whether a defined parametric threshold has been triggered. This determination is made post-event, giving both the protection buyer and ILS investor certainty as to the quantum of pay-out. The short-tailed nature of the product is what makes it appealing to investors, with no residual uncertainty or protracted settlement process. A trigger that responds to a defined period of cloud outage at a specific service provider would be an example of a cyber parametric trigger.

Industry loss indices for cyber catastrophe events have been available

[4] https://purplesec.us/resources/cyber-security-statistics/#Cybercrime

since 2017 and appeal to some ILS investors, many of whom already understand the concept from industry loss warranty (ILW) products traded frequently in the property catastrophe market. The loss development tail over time for cyber events in the collateral release mechanisms of these contracts, is an issue to address upfront. The goal is to strike a balance between buyers' need for protection and sellers' need to free up collateral after an appropriate length of time post-event.

UNL is perhaps the most challenging for cyber ILS instruments. The buyers' attraction to this trigger type is self-evident: risk transfer with high confidence that the pay-out will match actual losses incurred is preferred. ILS investors, however, may be circumspect for a few reasons.

Firstly, for the uninitiated, there can be a misconception that cyber coverage is ill-defined or amorphous. The reality is very different, however. Cyber insurance policy forms have matured over time with a convergence of standardised heads of cover offered in most products. With twenty years of loss experience behind it, the industry has clarified intent and evolved coverage over time. Key exclusions are also becoming more standardised, particularly for systemic events like war, critical infrastructure failure and state-on-state cyber operations.

Secondly, some ILS investors may be dissuaded by the longer loss development tail of third-party liability (TPL) claims. While TPL losses can take longer to fully develop than first-party losses, historical large cyber events have typically exhausted their cyber insurance programmes quickly due to sizeable first-party elements of the loss; third-party elements were therefore limited components of the overall loss quantum. Cyber insurance is typically written on a claims-made basis which naturally reduces the development tail for all losses, both first and third party. With certain limitations, negotiated collateral release mechanisms can enable capital to be freed up efficiently.

Ultimately, the extent to which the ILS community embraces each of the three trigger types will depend on several factors. Education about cyber risk and the underlying coverages is key for new investors, and due diligence will take time. Price is obviously paramount: protection buyers will expect a discount over UNL pricing in return for accepting the basis risk associated with parametric and index products, which might fall short of sellers' expectations, even in a hard reinsurance market. The cyber insurance market is set to continue growing and the insurance market penetration is increasing in established and emerging markets alike. There are limits to traditional market capacity to take on this extra demand and each of these cyber ILS triggers have a role to play.

Systemic risk understanding

The 2017 NotPetya attack is the closest there has been to a cyber catastrophe. Economic losses were approximately US$12.5 billion[5] (in 2022 US$) arising from the devastating malware, which deleted data and crashed systems among multiple global companies, including Maersk, Mondelez and Fedex. Most of the losses were either uninsured, or not covered by dedicated cyber insurance policies. This demonstrated the potential for catastrophic losses and focused the minds of cyber exposure management and modelling teams across the insurance industry.

Investors are most open to potential investments where the realistic disaster scenarios (RDS) have three specific characteristics: firstly, scenarios which can be as clearly defined as possible at the point of transaction; secondly those which can be ring-fenced post event; and finally, those which have a rapid resolution from a claims settlement perspective. There is growing convergence within the cyber insurance community, with support from regulators[6] on the type of events which are most likely to impact the industry

[5] https://www.brookings.edu/techstream/how-the-notpetya-attack-is-reshaping-cyber-insurance/
[6] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2021/august/insurance-stress-test-2022.pdf; https://www.eiopa.europa.eu/media/news/eiopa-consults-cyber-component-its-insurance-stress-testing-framework_en

in terms of frequency and severity of cyber-related losses. Three categories of catastrophe event are most common in how they are assessed by regulators and portfolio risk managers. They are:

- widespread data breach at a critical technology provider, such as an electronic payments service
- malware attack (which could include ransomware) on a key supply chain software provider
- cloud services outage (disabling access to critical services by users)

These scenarios, though necessarily reductive in nature, distil an infinite set of permutations of potential threat actors, threat vectors and outcomes into a digestible format which can be analysed and compared both between scenarios and over time. The intent is to create relative benchmarks for comparison between portfolios, as well as create a common lexicon and understanding of the risks between counter parties. One major source for improving the understanding of systemic risk has been the investment and development in cyber catastrophe models, which have now been scrutinised over several years and are growing in acceptance.

Model maturity

Some ILS investors have had the view that cyber (re) insurance losses are intrinsically un-modellable and that cyber underwriters lack the means to adequately quantify the risk. In addition to data collected by (re)insurers, there has been undeniable progress in the methodology and data which support cyber risk catastrophe models. Initial models were somewhat simplistic and deterministic, based on top-down aggregated market share data regarding the scope of a potential event. Cyber modelling has evolved in how it defines cyber events, creating clear differences between cyber perils, and adjusting modelling methodologies accordingly. In recent years, improved scanning technology and data capture has helped build credible datasets that identify dependencies between companies and the technologies they rely on.

Models are now able to display statistical analysis based on actuarial probabilistic techniques to show a range of potential outcomes, effectively illustrating insured exposures. A more focused scenario set has developed, based on market demand, which reflects the key priorities of cyber (re)insurers. They have also evolved to reflect new insurance products more closely and the specific types of costs which are covered. A structured approach to analysing the potential frequency, footprint, scope of impact and severity provides a repeatable and scalable model for the market and ILS investors.

There has been a big effort to educate potential investors, who typically are not specialists when it comes to cyber risks. Building confidence and credibility in the models being used is a keystone to the acceptance by investors in the thresholds at which exposure attaches, and associated pricing. The conversations are framed in the vocabulary of traditional catastrophe management, and a lot of progress is being made. There is now a growing critical mass of investors who are looking for new ways to benefit from different types of catastrophe risk securitisation.

Ongoing investment in cyber catastrophe models continues and the update development cycle is shortening. One area of focus over the next couple of years is moving from a range of individual cyber catastrophe events to umbrella categories of cyber catastrophe event types, which captures a broader set of groupings. For example, “cloud outage” and “operating system malware” represent a family of cyber events that occur at the same single points of failure, and the trend is that this methodology will likely expand across all cyber perils in each scenario catalogue.

Another area of focus is the need to adjust the modelled outputs to reflect changing cyber insurance terms and conditions, such as how systemic exposures are addressed in the primary policy. There is inherent uncertainty in any model for any peril, but with a transparent approach, together with clear definitions and simple structures, cyber models are fit for purpose to support investment trades. The cyber perils and scenarios being modelled can be explained using an understandable framework to give clarity for both parties to a trade. As with natural catastrophe frameworks, cyber models include assumptions around the frequency, footprint, and severity of events that are used to convey

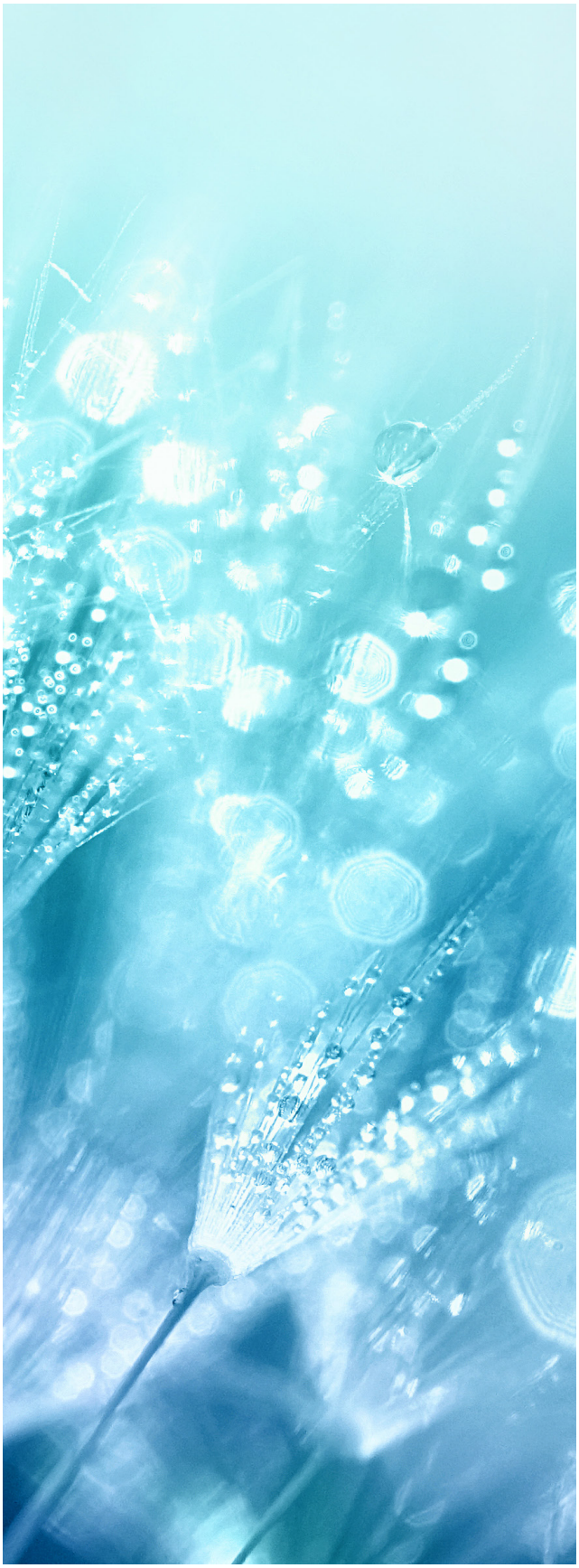
possible financial loss outcomes. Being transparent around how these assumptions are made, and where areas of increased uncertainty lie, is crucial to building a tradable investment vehicle.

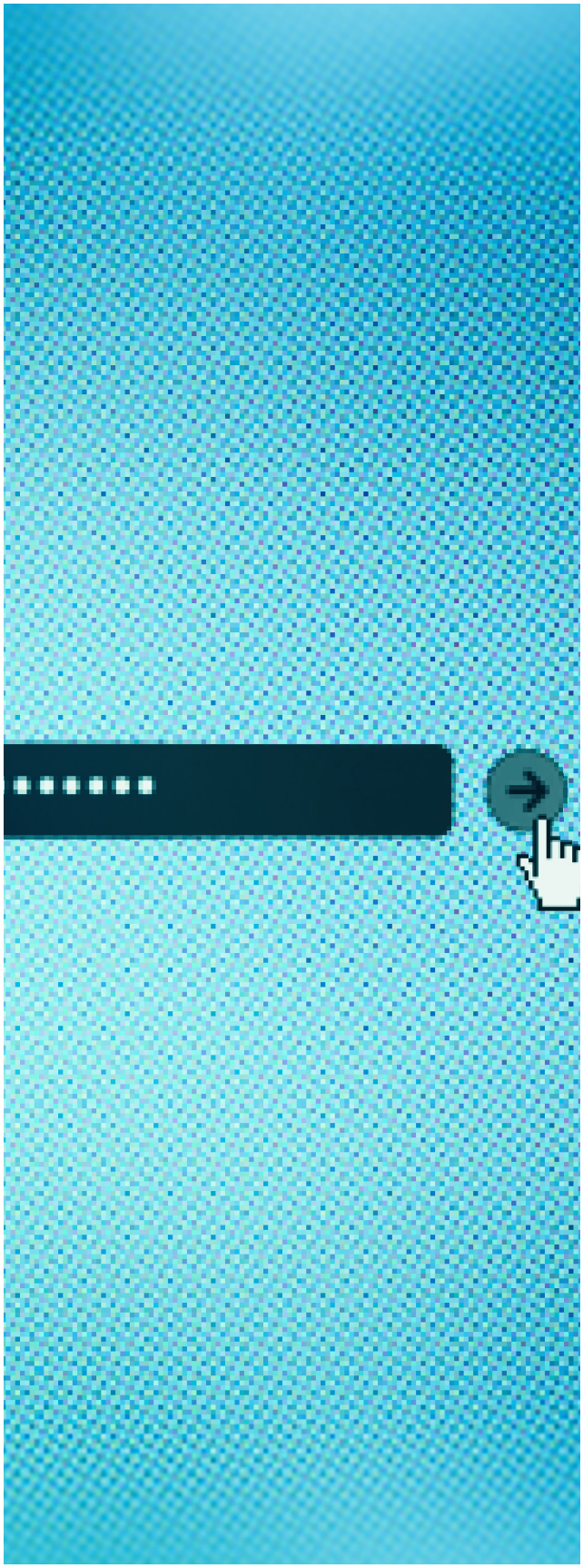
Correlated risks?

Another concern raised by ILS investors has been the perceived correlation risk that a cyber catastrophe could have with other financial systemic risks relating to the equity and debt markets. A major benefit of traditional ILS instruments, such as catastrophe bonds covering natural perils, has been the often-referenced diversification that they bring to an investment portfolio. The conventional wisdom suggests that an economic downturn or other financial shock has little correlation with the likelihood of a hurricane (or another natural catastrophe) occurring. For certain categories of natural peril, there are limitations to this concept of non-correlation between financial markets and physical hazard. There are extreme events that could directly cause material downturns in stocks and bonds. A magnitude 8 earthquake in the San Francisco Bay area or a Category 5 hurricane in Manhattan would be two such examples. Indeed, following the Tohoko earthquake and tsunami in Japan in 2011, the Nikkei index fell 11%[7]. There was also a significant drop in markets around the world following the global lockdowns at the start of the COVID pandemic.

Given the relatively short history of cyber insurance compared with property insurance, there is insufficient data to examine empirical correlation between cyber losses and major asset classes over a long timeframe. In the extreme tail of a loss distribution, there are hypothetical RDS in the cyber world that have a causal effect on stocks and bonds. Points of technology failure exist that could, in theory, produce insurance losses for thousands of policyholders, should these points ever succumb to a successful cyber-attack. The consequences for both cyber losses and financial markets could be extensive. For the correlation argument to hold up, it requires the assumption that such a systemic cyber event is so severe and long lasting that its impact is felt across industries and geographies.

These types of events (both for physical and cyber risks) are therefore extremely rare. We have a long period of





observation to be reasonably confident of this assertion for property cat events (although the picture is muddied by climate change). For cyber events, we have a shorter period of observation, but there are many other factors to provide comfort here. A vulnerability requires exploitation by malicious actors to be impactful before patches are deployed by companies. Known vulnerabilities are typically scanned and patched promptly, and the key technological points of failure are well-resourced enterprises such as major cloud providers with impressive cyber resilience. Threat intelligence is also rapidly evolving to identify new and changing cyber risks, which enables businesses to tackle potential attacks.

> "Core components of internet infrastructure are not built on uniform technology, which means global cascading attacks are an extremely remote possibility. It does not consider the increasing resilience and experience in responding to these types of events."

The growing enterprise adoption of cloud-based infrastructure has encouraged segmentation between networks and increased redundancy, which reduces the likelihood of contagion by a major event.

(Re)insurance companies themselves are also playing an active role in this area with the growing provision of ongoing threat-monitoring services to their policyholders, managing risk in real-time (or near real-time) rather than simply providing indemnification after the event. Within the policy coverage itself, war exclusions, first borrowed from other

[7] https://www.nytimes.com/2011/03/16/business/global/16iht-markets.html

> Exclusionary language removes several sources of systemic risk and therefore reduces correlation with other financial asset classes.

insurance classes, have been tailored to address the nuances of cyber insurance. The Lloyd's Market Association (LMA) has promulgated standard exclusions that Lloyd's looks set to mandate for syndicate-wide adoption in April 2023, which exclude or materially limit coverage for state-on-state cyber operations. Other insurers are adopting similar approaches in their own policies, as the market coalesces around best practice in this area.

Beyond war exclusions, critical infrastructure exclusions are prevalent, encompassing disruption to utilities, electrical and mechanical services, core internet infrastructure (such as cabling and related hardware) and other telecommunication services. Consequently, some RDS would not be covered under cyber insurance policies – for example power outages induced by a cyber-attack. Others would be sub-limited or subject to a specific policy deductible. All this serves to mitigate catastrophic risk potential which should dilute correlation with financial asset classes.

One other factor is the human element. The multi-layered motivations of threat actors, be they financial, political, or ideological in nature, are mirrored by the efforts to mitigate the effects of an event in real time by the cyber security and insurance community. These can significantly reduce the impact of an event (for example the WannaCry malware of 2017 was stopped in its tracks when its "kill switch"[8] was identified by a security researcher). Financial markets can interact with these threat types in complex ways, and it would be naïve to say returns from cyber (re)insurance and other asset classes are completely independent. However, the case for strong correlation between cyber and other financial asset classes is weak, with the exception for both cyber and property catastrophe risk in the extreme tail of the distribution. The thesis of diversification is valid. For medium to longer term investors, cyber risks should be seen as an alternative, diversifiable asset class, in much the same way as natural catastrophe risks. If short-term correlation occurs, with investor reaction to a cyber event creating heightened market volatility, this dissipates once the magnitude of the actual losses become more transparent.

Turning data into insight

Back in 2006, the phrase "data is the new oil" was first attributed to British mathematician Clive Humby. More than 15 years later, this analogy has broadly held up, as unless its potential is harnessed through refinement and product innovation, the raw material of data has limited value in its unrefined state. ILS investors raise concerns that there is insufficient data to calibrate cyber loss models. Yet policies today provide cover across all industry verticals to a diverse range of insureds on every continent, and over 20 years' worth of exposure and loss data exists with which (re)insurers can inform their view on cyber risk. In the initial stages of the market, insurers partnered with the reinsurers, using quota share reinsurance to transfer and share risk. With a direct look-through to each underlying claim and policy subject to the quota share contracts, first movers in cyber treaty reinsurance were able to build comprehensive data spanning much of the market. Cyber risk is inherently data-driven and many aspects of it have a digital footprint. The best operators in the space have built mature analytical capabilities powered by this data, with machine learning, data science and statistical methods able to quantify loss potential.

One area where there has been progress, though still plenty of work to be done, is in the quality of the data collected by (re)insurers themselves. This makes it easier for ILS investors to understand and support the market. There have

[8] https://techcrunch.com/2019/07/08/the-wannacry-sinkhole/

been improvements in the granularity of data to capture specific data fields at the point of underwriting relating to technology supply chain, operating systems, and other indicative variables, providing the insights and transparency to make better informed decisions. Long term data strategies are emerging within the cyber insurance industry to deliver continued improvements in data quality for use in the quantification of cyber risk.

Another concern often raised by ILS investors is that, even with extensive data sets, it is impossible to quantify cyber risk to any degree of precision due to its dynamic and ever-changing threat landscape. There are inherent challenges in assessing catastrophic cyber threats, in that the tools, techniques, and procedures of the threat actors change frequently. It is a constant tug of war between attackers and defenders of networks. As a result, historic loss data is less valuable to (re)insurers assessing the frequency and severity of risks compared with more stable perils. It is true that this state of flux is one of the biggest differences between property catastrophe risk and cyber. While earthquake and hurricane risk remain relatively steady over time, cyber risk appears chaotic and unpredictable. The reality, though, is very different. Cyber is an anthropogenic peril which is the very thing that makes it predictable. Humans are motivated by incentives. Distinct threat actors are at play (cyber-criminal groups, nation states, hacktivists, ... etc.) and, in most cases, their incentives are known. Their intended targets can be anticipated, as are their preferred attack patterns and likely attack vectors. Intelligence on these threat actors, methods and targets is actively reported via structured data disseminated by the cybersecurity community. Successful cyber-attacks and many failed attempts (so called "near-misses") are known. Trends in this data can be identified and models can be recalibrated accordingly, with machine learning techniques particularly well-suited to handling this workload and able to keep up with the pace of change.

There is no shortage of cyber security data sources available, such as network scanning, supply chain tracking, and end point detection and response software. The challenge is leveraging the right combination of data to turn it into insight, so that better decisions around capital deployment can be made. Building an ecosystem of data providers across different categories provides a substantial lift on the accuracy and precision of the outputs.

> By combining data such as that relating to cloud outages, external network scans, internal risk management processes, exposure and claims, better insights can be brought to the challenge of representing the potential cyber catastrophe losses, which ILS seeks to address.

Some of the volatility which has been evident in cyber cat modelled tail risk results has been the result of the ongoing evolution and calibration of models as the risk is better understood, rather than a true reflection of dramatic changes in the actual risk landscape. Deep insights can be extracted from those in possession of data to quantify cyber risk. Modelling tools are calibrated to assist in the underwriting and portfolio management of profitable cyber risks on behalf of ILS investors.

Addressing questions of collateral

Given the nature of collateralisation, there is a structural tension that exists in ILS transactions between the protection buyer's desire to ensure that collateral remains available while the ultimate loss amount is determined (and subsequently paid out), and the investor's desire to withdraw excess collateral as soon as possible. This tension exists regardless of the ILS instrument and line of business. Ultimate losses for any event cannot be known with certainty until sometime after an event (of any type). For example, Hurricane Irma underwent significant loss creep with ultimate loss estimates increasing substantially in the years following.[9]

Worst case scenario for the protection buyer would be to release the collateral too early and then experience adverse loss development with no clawback provisions. Equally, the investors would potentially have collateral trapped needlessly for extended periods of time, with no ability to redeploy it elsewhere, thereby reducing returns. Somewhere between these two positions is a compromise. Analogies can be drawn from the structures and mechanisms used in property cat ILS transactions to see how they can be reshaped for cyber ILS deals. Mechanisms such as so-called "buffer loss tables" with agreed tapering over time can be used to allow for uncertainty in the ultimate loss value. This still allows for collateral to be released over a relatively short period of time, whilst maintaining ring-fenced funds for the buyer's benefit until the contract is commuted.

These mechanics can be modified in a few ways to accommodate cyber perils. One complexity to address is the mix of short tail first-party exposure (such as business interruption and ransomware payments and recovery costs), as well as the longer tail risks related to liability and regulatory risks associated with privacy breaches. To address the variety of cyber losses, especially if an event occurs towards the end of a contract, a grace period following the contract could be included, during which time the buyer has the option to hold all the collateral. Additionally, the buffer loss table schedules often seen in private collateralised (re)insurance transactions could be altered so the buffer factors taper off more slowly. This recognises the longer-tailed nature of some cyber losses and helps support a more cautious cyber ILS market. There are also nuances in that different buffer factors could apply to first-party and third-party claims, recognising inherent differences in their respective development tails.

[9] https://techcrunch.com/2019/07/08/the-wannacry-sinkhole/

Finally, incentives could be introduced for both protection buyers and sellers. The protection buyer could be required to pay interest on outstanding collateral balances after expiry of the contract (and any grace period). There is precedent for this already in securitised property cat bonds and growing support in other forms of collateralised risk transfer. This would incentivise the protection buyer to release collateral promptly and not to unnecessarily increase ultimate loss estimates. Another incentive is to introduce a no claims bonus in the reinsurance structure design, payable only if the contract is commuted within a stipulated timeframe following expiry. While this does not guarantee early collateral release, it would likely incentivise the protection buyers in cases where a reinsurance recovery looked highly improbable. There is already precedent for such mechanics in cyber excess of loss (XL) deals, in particular event XL and aggregate XL treaties. There are additional roles for fronting partners in the transformation of risk, with several levers which can be borrowed from the property cat ILS world and tailored to cyber reinsurance, while safeguarding the interests of both protection buyers and sellers.

Exceeding the Returns Hurdle

One reservation from investors relating to ILS investments in emerging risks such as cyber, has been the challenge of a market clearing price to be achieved. Even within property catastrophe risks, price expectations for ILS investors have been harder to sustain, given the previous abundance of traditional reinsurance capacity. However, after several years of falling rates within property reinsurance, traditional reinsurance pricing has increased since 2019 due in part to the cumulative impact of multiple natural disasters in the 2015 – 2019 period. A situation which became more acute during the 2022 / 2023 renewal season. This has had the effect that the per unit pricing of rated reinsurance capacity is now much closer to the expectations of ILS investors. Additionally returns for ILS investors in the property cat segment have stalled, given the number of natural disasters in recent years (see Figure 4).

Within this context, the original cyber insurance rates have increased even faster than other lines of commercial insurance since 2019, primarily due to increased ransomware losses. They have more than doubled in cyber insurance

> "The increases in cyber insurance are not driven by cyclical factors such as withdrawal of capacity following a specific loss event, but rather should be viewed more as a pricing correction and stabilisation."

since 2020[10] . Notwithstanding a recent moderation of cyber insurance rate rises, reinsurance rates continue to increase. Unlike other classes of insurance, cyber catastrophe risk pricing and an improved understanding of the risk landscape, as well as increasing underwriting discipline have been the primary drivers of this re-pricing. All of this has created a more compelling view that rate adequacy is being achieved for taking on cyber risks. There is a better understanding of what constitutes rate adequacy.

Another factor which is creating some convergence over return thresholds, is the macroeconomic headwind relating to growing fear of recession in many western economies. This is creating downward pressure on current equity returns. One counterpoint to this trend is the increase in interest rates from major central banks, such as the Federal Reserve, the Bank of England, and the European Central Bank, to tackle inflation. Although inflation creates challenging conditions for a variety of reasons, many forecasts[11] estimate that interest rates will peak by mid-2023, based in part on other factors which will ease the inflationary trend. As a result of these factors, expectations of returns for ILS investors are closer to being met or exceeded.

[10] https://arcticwolf.com/resources/blog/real-causes-cyber-insurance-rate-increase/
[11] https://tradingeconomics.com/forecast/interest-rate?continent=america

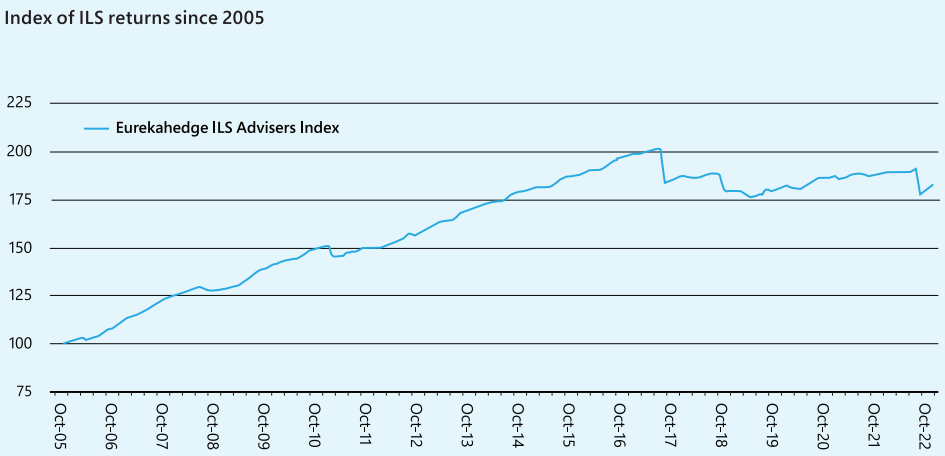


Figure 4. ILS returns have stalled in the last few years due to increased natural catastrophes

Market clearing on the horizon

The recent news that Beazley Group has launched a private cyber catastrophe bond[12] utilising CyberCube's catastrophe model is an encouraging sign of progress in this area. It demonstrates that the efforts are beginning to bear fruit. There is a concerted ongoing engagement to educate investors on how cyber models, coverage, and risk management operate, providing cyber specific underwriting support. The perception that cyber risk is unquantifiable is reducing, and more investors are getting comfortable with the level of specificity which can be established for cyber perils.

> The mechanisms and methodology behind cyber modelling are becoming better understood, and the strength of the data and frameworks being utilised is growing all the time. All of this creates an environment where the potential for cyber ILS investments can be leveraged to play a critical role in unlocking capacity required to continue developing the wider cyber insurance market.

This in turn supports more effective financial resilience in the face of ongoing cyber threats.

This paper makes the compelling case for cyber ILS, having addressed the common objections. The massive opportunities which arise from the continued demand for cyber (re)insurance will only be further enhanced by the successful execution of cyber ILS transactions. This will increase (re)insurance capacity, as well as isolate cyber catastrophe risk into a tradeable format. There is an acknowledgment, that as in any new category of investment, progress may be incremental, relatively small scale at first, and slow. The early trades may be harder to execute, but once those innovators seize the first mover advantage, there will be many following on. For now, in 2023, the ingredients are there for momentum to grow.

[12] https://www.insurancebusinessmag.com/uk/news/cyber/beazley-reveals-markets-first-cyber-catastrophe-bond-432289.aspx

Authors:

Oliver Brew
Lockton Re Cyber Practice Leader
oliver.brew@lockton.com

Zach Breslin
Lockton Re Capital Markets Leader
zbreslin@lockton.com

David Ross
Envelop Risk Executive Vice President of
ILS & Capital
david.ross@enveloprisk.com

Brittany Baker
CyberCube Vice President of Solution Consulting
brittanyb@cybcube.com

Yvette Essen
CyberCube Analytics Head of Content,
Communications and Creative
yvettee@cybcube.com

Contacts:

Isabella Gaster
Lockton Re Global Head of Marketing
isabella.gaster@lockton.com

Elizabeth Miller Kroh
Lockton Re Head of Marketing, North America
elizabeth.kroh@lockton.com

Designers:

Anna de Souza Morgan
Lockton Re Senior Designer
anna.desouzamorgan@lockton.com

Rachel Clarke
Lockton Re Graphic Designer
rlclarke@lockton.com

Addresses:

New York

48 West 25th Street, 7th floor
New York, NY 10010
United States
Office phone number +1 646 572 7300

United Kingdom

The St Botolph Building
138 Houndsditch
London EC3A 7AG
United Kingdom
Office phone number +44 020 7933 0000

Legalities:

Please note that our logo is Lockton Re; our regulated entities are Lockton Re, LLC in the USA Lockton Re, LLC, 48 W 25th Street, New York, NY 10010 and Lockton Re LLP in the UK Registered in England & Wales at The St. Botolph Building, 138 Houndsditch, London, EC3A 7AG. Company number OC428915.

Lockton Re provides this publication for general informational purposes only. This publication and any recommendations, analysis, or advice provided by Lockton Re are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. It is intended only to highlight general issues that may be of interest in relation to the subject matter and does not necessarily deal with every important topic nor cover every aspect of the topics with which it deals. The information and opinions contained in this publication may change without notice at any time. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Lockton Re shall have no obligation to update this publication and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as reinsurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your applicable professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the information contained herein could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. This publication is not an offer to sell, or a solicitation of any offer to buy any financial instrument or reinsurance product. Nothing herein shall be construed or interpreted as a solicitation of any transaction in a security or commodity interest as defined under applicable law. If you intend to take any action or make any decision on the basis of the content of this publication, you should seek specific professional advice and verify its content.

Lockton Re specifically disclaims any express or implied warranty, including but not limited to implied warranties of satisfactory quality or fitness for a particular purpose, with regard to the content of this publication. Lockton Re shall not be liable for any loss or damage (whether direct, indirect, special, incidental, consequential or otherwise) arising from or related to any use of the contents of this publication.

Lockton Re is a trading name and logo of various Lockton reinsurance broking entities and divisions globally and any services provided to clients by Lockton Re may be through one or more of Lockton's regulated businesses.


LOCKTON
REINSURANCE


CyberCube


envelop
progress secured