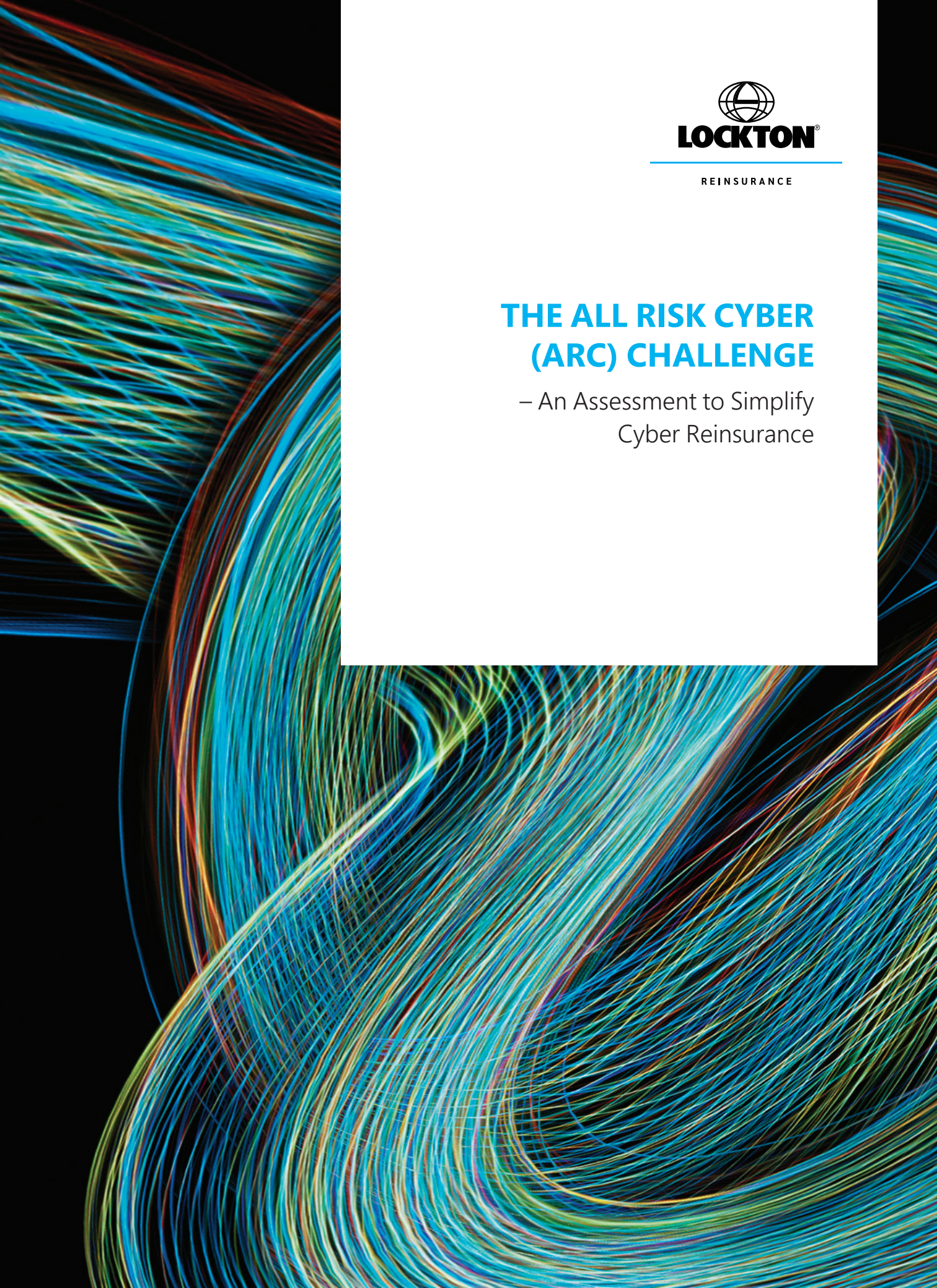


LOCKTON®

REINSURANCE

THE ALL RISK CYBER (ARC) CHALLENGE

– An Assessment to Simplify Cyber Reinsurance

HELPING BUSINESS UNDERSTAND, MITIGATE AND CAPITALISE ON RISK

Executive Summary

Cyber security needs a rebranding. It encompasses images of hackers, Artificial Intelligence (AI), and an alphabet soup of buzz words that fill industry headlines and conference agendas.

Cyber insurance suffers from a similar ailment. Much discussed, much maligned, cyber insurance confounds an insurance industry focused on simple categories of First Party and Third Party risks by combining these elements into a single product. Cyber exposures are not easily placed in a category or peril framework. The insurance industry has divided itself, for the sake of sanity, into Short(ish) and Long(ish) tail[1] business of similar perils. In its most basic form: have assets been damaged or stolen? Is there potential liability or the threat of a lawsuit/class action? The Cyber insurance product muddies that bifurcation. We contend this is an accident of history.

The original insurance buyer wanted a simple solution to a complex problem: the result is the current All Risk Cyber (ARC) product which supports 1) First Party (Shortish) perils, 2) Third Party (Longish) liabilities, as well as relatively recently identified 3) Catastrophe or Systemic severity exposure. These three elements challenge an industry that was designed to fit products into simple categories. Lockton Re's Cyber Centre (LCC) contends that the problem is not the insurance industry's lack of adoption to the ARC product, but that ARC, at least from a reinsurance perspective, is not the optimal solution currently and into the future.

The ARC problem limits the supply of capital and the insurance industry's ability to scale cyber insurance in a sustainable way. Currently, original buyers of the cyber insurance product feel limited in the scope and scale of market where buying is usually straightforward: protect assets from damage (whether tangible or intangible) or defend against liability in exchange for a premium. In mature classes of commercial insurance where First and Third Party risks are broadly separated, billions of dollars of capacity are available to support demand. Within cyber, these two elements create an original sin by commingling protection types for largely a single cost. Our contention is that splitting out the perils into their constituent parts will enable more effective risk transfer to reinsurers, and further down the value chain (retro/ILS) capacity in a more targeted and scalable fashion.

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

[1]Short and Long Tail refers to the claims development pattern; in this instance to the length of time claims take to manifest. A fire happens quickly (short tail of claims development) an oil leak causes an environmental damage claim over a period of 10–15 years, resulting in a claim 15 years or more after installation (long tail of claims development).

Cyber insurance market – why people won't stop talking about it

For 25 years the debate has raged that the cyber insurance market has not yet fulfilled its potential. Take-up rates[2] are still lower than other specialty products, particularly given the risks at stake. The beginnings of the market had one common theme: underwriters and brokers largely worked in Third Party Professional Liability (PL), otherwise known as Errors & Omissions (E&O). The Information Technology (IT) boom created liability risks for large technology companies as they grew, and internet technology emerged. Many of the structures of an E&O policy carried over into the early cyber insurance policies, and the hallmark of this heritage is still evident today in the policy language and coverage offered. Errors and Omissions underwriters and lawyers used familiar templates to develop the first generation of cyber policies.

> "Many of the structures of an E&O policy carried over into the early cyber insurance policies, and the hallmark of this heritage is still evident today."

As an example of the borrowing from the familiar, policies are typically written on a "claims made" basis with extended reporting provisions, and other clauses directly lifted from E&O policies. The applicable coverage is based on when the claim is made (or loss discovered) during the policy period, rather than when the loss first occurs. Another legacy of the E&O influence on the history of cyber insurance is the broad application of privacy liability principles – which still resonates today. The seedling of the current cyber market was that a major concern at the time was about the potential liability associated with a company passing, unintentionally, malicious code to a trading partner or customer. This became the focus of the early policy language and embedded Third Party liability in the core of the offering.

The dramatic explosion of the internet exponentially increased the peril that was not initially adequately addressed by the insurance industry. Many existing property and casualty policies simply did not address risks associated with computer systems or data. The axiom that the insurance industry drives by looking in the rear view mirror, rang true. As the realisation of unintended exposure grew, "data exclusions" and similar clauses were hastily drawn up for standard policies to limit risks which were neither priced for, nor underwritten to, including the millennium bug[3], which was excluded from most policies. Early primary cyber insurance policies expanded in scope to try and catch up with the rapidly evolving technology, and specific First Party covers emerged to address new risks.

[2]https://www.leasinglife.com/features/cyber-insurers-price-out-smes/?cf-view
[3]https://education.nationalgeographic.org/resource/Y2K-bug/

Blending First and Third Party risks – the beginning of an All Risk Cyber (ARC) Solution

As the fledgling market emerged and grew in the 2000s and early 2010s because of increasing cyber-attacks and digital criminality, it became clear that data breach response cover, business interruption and related First Party perils were key components of the coverage.

For most insurance carriers, cyber insurance policies incorporate a mix of First Party and Third Party covers. These heterogeneous risks have become bundled into a single product over time. Short tail risks have specific characteristics in an insurance context, in that where losses are addressed promptly. This enables capital to be repurposed efficiently to take on new risks. By contrast, Third Party liability claims can inherently take a much longer time frame to settle, due to the legal processes and timelines involved. Long tail risks are handled differently from an actuarial reserving perspective, and require close monitoring to manage any adjustments in potential defence costs involved, interaction with regulators, offers of settlement, litigation timeframes and similar.

> There are very distinct differences in how First Party and Third Party risks are handled in the insurance value chain.

There are very distinct differences in how First Party and Third Party risks are handled in the insurance value chain. Underwriting, claims and reserving all require separate methodologies, experience and data. The evolution of cyber insurance is such that these varied risks have become commingled into a single product. This creates complexities in how the risk is handled, processed, and ultimately how capital can support each category of risk. Untangling the different strands of cyber perils within the reinsurance market provides a huge opportunity to increase participation in the market, unlocking the supply of capital and supporting the growth of the wider market to meet continued demand.

Improving the understanding of catastrophic risks

As the connectivity and dependency between companies and global networks has grown, it has become increasingly clear that there is the potential for widespread exposures across a portfolio of insured risks. The so-called "cyber hurricane" was an early moniker which was shorthand for a wide range of different types of catastrophic risks, including cloud outages, supply chain malware attacks, and the exploitation of vulnerabilities in common software components. A consensus[4] has slowly emerged around a key set of realistic disaster scenarios. These include:

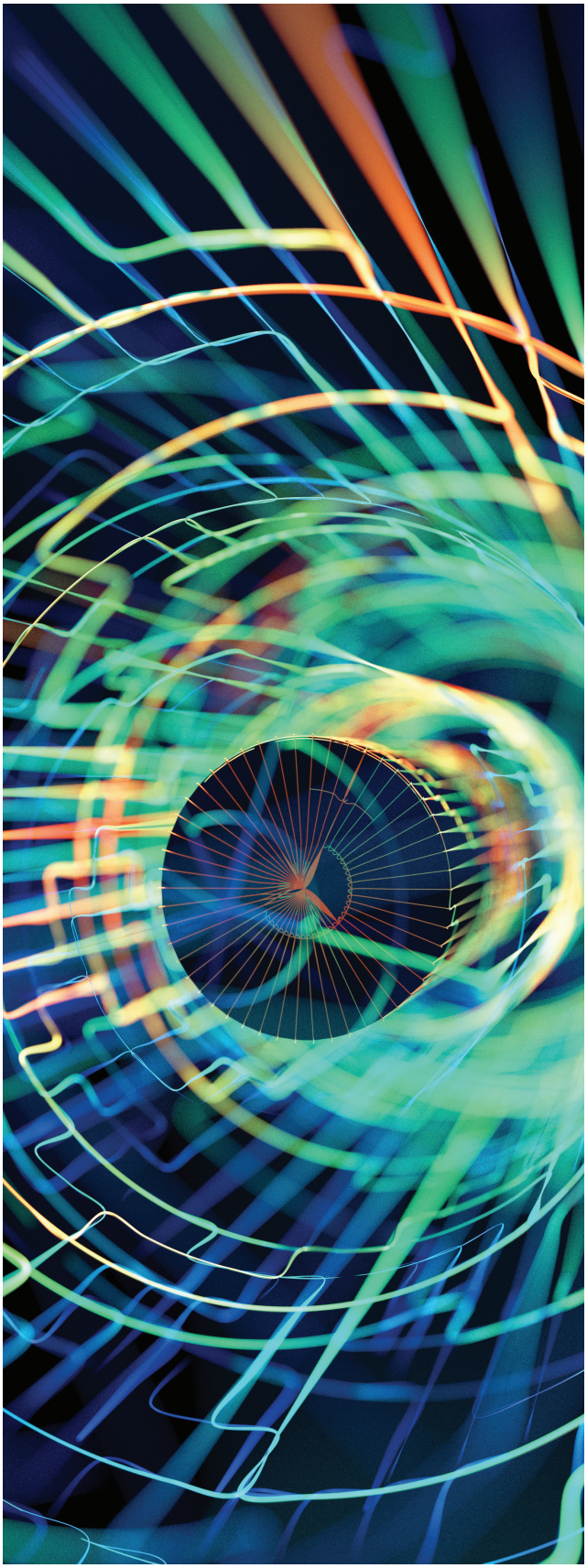
- widespread malware event (such as the 2017 NotPetya attack)
- widespread data breach event (such as the 2015 Anthem Healthcare)
- mass cloud outage (such as the MS Azure outage in early 2023)

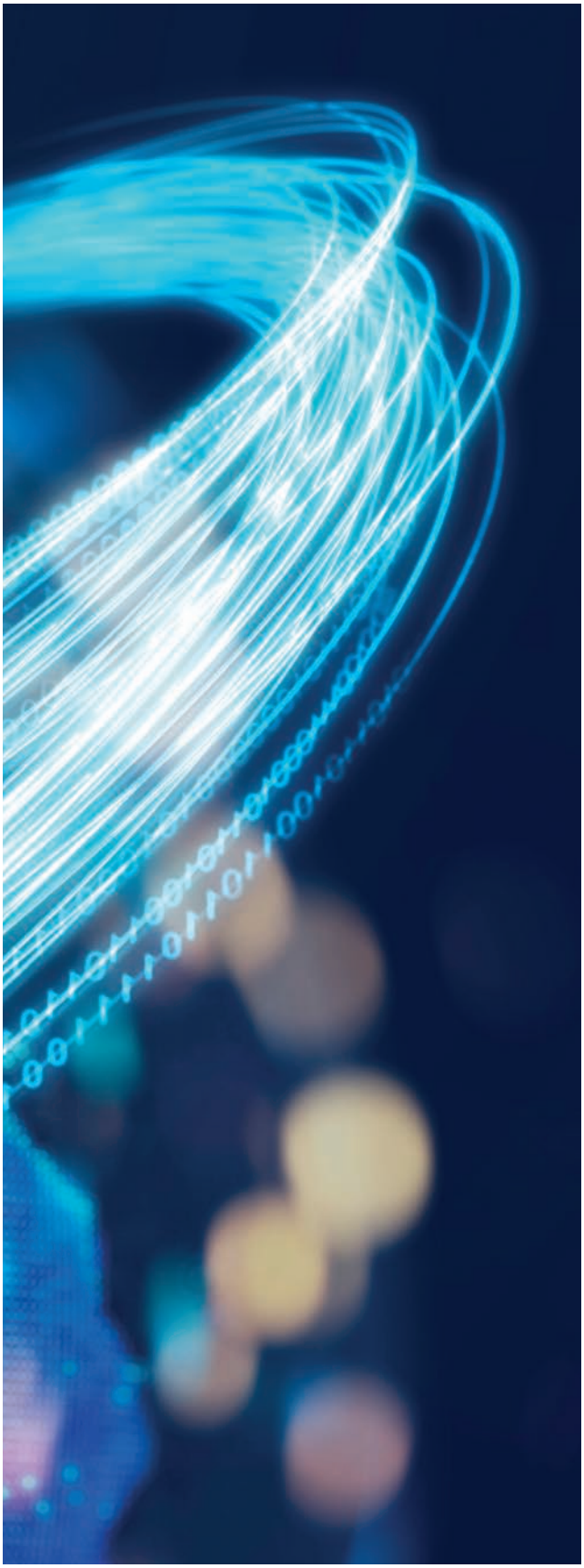
There are innumerable permutations of these events, but these provide a sense of scale about how bad a catastrophic event could be. Of course, given the scarcity of recorded catastrophes, forward-looking models have contended with skepticism and are slowly gaining market confidence and credibility. With growing understanding, models enable a common language to transfer catastrophe risk into the private market, such as with natural perils (earthquake and property catastrophe).

[4]https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2023/thematic-findings-2022-cyber-stress-test.pdf

In recent years, there has been an increasing awareness and focus on the potential for systemic risk, and its impact on the cyber insurance market. Catastrophic risks, in which multiple companies can become victims of the same cyber event, manifest in different ways. There are two main areas where the use of exclusionary language is intended to limit the market's exposure to unmanageable catastrophic risk: firstly, critical infrastructure and secondly, war. The failure of core infrastructure which supports the internet, such as domain name service providers, internet service providers or power generation, could have vast consequences. Similarly, conducting war between nation-states or non-state actors, via digital means, is also an issue which has brought systemic risk into sharp relief with the advent of the Russian invasion of Ukraine. In common with all other commercial insurance lines, war is broadly accepted as beyond the scope of the private insurance market. The nuance of the language required to reflect the intent is not something addressed here, suffice to say that the reinsurers play a central role in driving adoption of a common approach to the issue.

Lessons can be drawn from the Natural Perils Catastrophe reinsurance market, and there is an evolving category of cyber catastrophe insurance product, which specifically addresses systemic risks. This makes it easier for reinsurers to accept specific types of catastrophe risk, within understandable parameters, just as is the case for physical property catastrophe risk. Models for these perils have developed over the last thirty years, and provide valuable insights and benchmarking to analyze and plan for natural catastrophe perils.





Enter reinsurance

The reinsurance industry supports the ARC product sold by primary carriers with broad reinsurance product structures such as Quota Share, Aggregate Excess of Loss, Per Risk, and Occurrence Excess of Loss solutions. The reinsurance carriers that support these products need to balance the short, sharp loss profile of the First Party elements, both of individual and potentially systemic events in the ARC product, with the long tail loss profile of the Third Party elements. Aligning capacity and capital to a shortish/longish loss profile is understandably difficult and has limited the reinsurance market's ability to transfer cyber reinsurance exposure further up the supply chain of risk (retrocession and capital markets).

The current All Risk Cyber (ARC) product is problematic for the reinsurance industry. As outlined above, the original product is an All Risk policy, in that it contains:

- Third Party Liability Peril
- First Party data breach, extortion, and Business Interruption product
- Catastrophe / Systemically exposed perils

Reinsurers' initial strategy to deal with this problem, like the original market, was to ignore the First Party perils and hope that the losses don't get too volatile or too big (unfortunately ransomware undermined this approach...). The strategy was then employed to separate cyber reinsurance underwriting teams from Casualty or Specialty units into specific teams, and hope that the Third Party liability does not get too big (unfortunately pixel tracking suggests this is optimistic). It has been a game of whack-a-mole with ever evolving cyber perils creeping up, and old ones coming back to haunt loss development.

The ARC Solution – breaking up the band – original cyber product continues in its current form, but the reinsurance solution adapts to:

1. Extract Third Party liability emanating from cyber insurance policies out of the cyber-specific reinsurance treaties and place it with casualty / liability focused reinsurance products.

2. Continue to purchase cyber standalone treaties on the First Party and Catastrophe specific exposures that exist within the original cyber insurance market– with a focus on the cyber peril and the business interruption/business continuity peril.

Immediate benefits:

1. Separating First and Third Party risk for reinsurance purposes allows clients to utilise two pools of intellectual knowledge and reinsurance capacity aggregate. Crucially, this allows access to more capital. The standalone cyber divisions and the Professional Lines divisions of reinsurance companies will have two separate loss development profiles and are established to support independent assessment.

2. Reserving of Third Party claims, due to the tail (length of reporting) and the latency in their development, extends the time over which an insurance premium can make an investment return.

3. First Party and systemic perils are short in tail (length of reporting) and manifest relatively quickly. A denial of service attack doesn't suddenly manifest two years after it is implemented. This allows additional short-term capital to support segments of the cyber peril without fear of years of loss development or trapped collateral.

4. Insurance carriers can have open and frank conversations with insurance buyers and brokers about the impact that risk controls have on the First Party and Third Party pricing for the original business. Rather than cyber hygiene as a general area of improvement, this focuses the conversation and enables more meaningful cost/benefit analysis to be conducted.

5. Shorter tail First Party perils mean that it will be easier to package and trade in the secondary and alternative market, encouraging more capital to participate in the market. The narrower reinsurance coverage means less tail risk uncertainty making it easier for additional capacity.

6. Bifurcation of First and Third Party perils should improve risk transfer in non-proportional programmes.

There are of course, some challenges to any transition into a different way of purchasing reinsurance. None of these are insurmountable, but continued innovation and progress within the insurance industry are required to overcome them. These include:

1. Some carriers do not currently capture premium data in a sufficiently detailed format to identify risk premium specifically associated with individual heads of cover, or even broad First and Third Party peril categories. Improvements are required to create a consistently high standard of premium data quality for widespread adoption.

2. Allocation of premium and exposure between different categories of risk is not internally consistent within primary carriers in a defensible manner.

3. Losses which involve both First Party and Third Party perils, will require pre-agreed allocation of losses to different coverages.

4. Reinsurer appetites may evolve at different speeds, creating potential challenges to fulfil primary carrier needs.

> When the risk is as dynamic as cyber, which is anthropogenic in nature and thus rapidly changing, insurance and associated risk mitigation is forever catching up with reality.

Playing catch-up

One challenge that all commercial insurance risk faces, is that policies are often written with past incidents and losses in mind. When the risk is as dynamic as cyber, which is anthropogenic in nature and thus rapidly changing, insurance and associated risk mitigation is forever catching up with reality. A striking example of this constant process of catch-up, was that when cyber extortion coverage was first included in cyber insurance policies, it was not rated for in the insurance premium and there were no specific underwriting questions. Extortion was considered a rare and remote threat, typically conducted by a disgruntled individual against their former employer.[5] Examples have included sacked IT or finance staff, who then sought revenge by threatening to release employee information. These incidents were relatively small scale and had limited impact. Coverage was offered as a "throw-in" without much additional consideration.

In the latter half of the 2010s, extortion as part of the cyber insurance product evolved from an afterthought to the most prominent coverage. In May 2017, the WannaCry[6] ransomware attack was extremely rapid in its spread. It caused mass encryption of operating systems for several hundred thousand computers. The ability to mitigate the impact was limited, and in some cases, ransoms were paid to release the decryption key. Ultimately, the fortuitous discovery[7] of a "kill switch" ended the self-propagating nature of the malware.

The NotPetya[8] attack also took place in 2017 and highlighted the value of forensic investigation and response coverage, as well as the potential impact of a widespread incident. Losses were paid under affirmative cyber policies, and there was much more significant (if unintended) coverage from property policies. As ransomware became an increasingly important concern for policy holders following this, cyber extortion (First Party) coverage came under a new spotlight.

Historic Cyber Events: Economic Losses[9]

Event	Year	Economic Impact (US$ Bn)
Nimda	2003	0.635
SQL Slammer	2003	0.75
Mydoom	2004	38
Sasser	2004	0.5
Conficker	2007	9.1
WannaCray	2017	4
NotPetya	2017	10

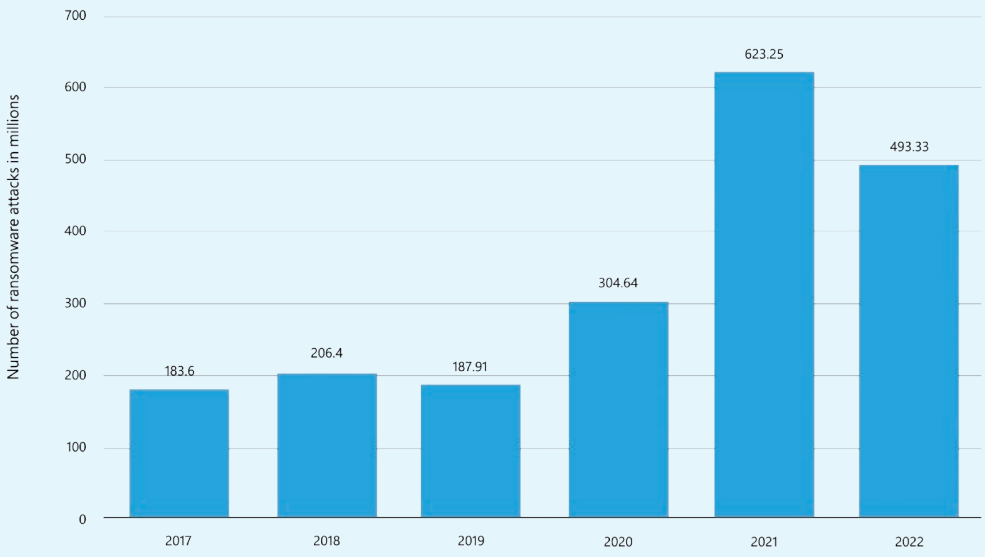
Source: Verisk

[5]https://www.kentonline.co.uk/weald/news/former-employee-targeted-firm-in-cyber-attack-putting-150-jo-250492/
[6]https://www.malwarebytes.com/wannacry
[7]https://www.ncsc.gov.uk/blog-post/finding-kill-switch-stop-spread-ransomware-0
[8]https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[9]https://www.verisk.com/siteassets/media/pcs/pcs-cyber-catastrophe-notpetyas-tail.pdf

Insured losses from WannaCry were limited but it began a trend, and between 2019 and 2021, extortion became the most prevalent cause of loss to the insurance industry. The losses incurred are short tail in nature and often require a response in hours, rather than days or weeks. This is due to the immediate negative impact that a ransomware extortion event can have on a business. A prompt reaction team may be needed to assess the malware, analyse the threat actor and their motives, and decide on whether and how a ransom demand is responded to. Ransom demands grew from hundreds of dollars to thousands and then millions. As losses increased in both frequency and severity, extortion related losses became the single largest source of claims for the cyber insurance industry. Threat actors evolved and ransomware now often includes data exfiltration, increasing the impact and cost of an event.

Ransomware has become one of the defining themes for cyber insurance in the last few years.[10] Malware has been ruthlessly exploited by hacking groups for substantial financial gain. It is also an asymmetrical threat, as the cost to hackers of conducting ransomware campaigns is relatively low, compared with the potential upside. Conversely, the effort to defend against the threat is high and hard to measure precisely. Today, both the cyber security and insurance industries have invested heavily to educate companies, raise cyber hygiene standards, and limit the damage caused by ransomware attacks. Dramatic underwriting actions have been required to enable cyber risk to continue to be insured. It was in a sense, an existential necessity for the industry to address the issue, as losses were haemorrhaging during this period. Strict limitations of coverage were introduced, tight new security controls required, and rates increased. At the peak of underwriting correction measures, there was an oft-quoted phrase which customers dreaded: "double, double, half": double the premium, double the retention and half the limit.

Annual number of ransomware attacks worldwide from 2017 to 2022 (in millions)



Source: SonicWall © Statista 2023

[10]https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/

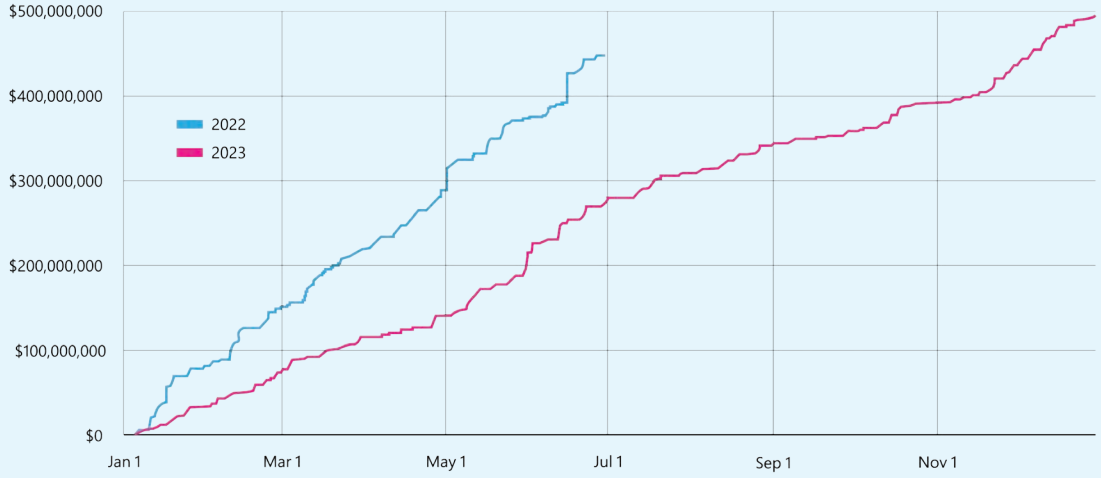
Cyber crime evolution

The evolution of cyber crime presents another significant challenge in the ever-changing world of cyber risk. It's clear that as the internet has become ubiquitous, previously neatly segregated perils, which were classified within a specific commercial insurance line of business, have now become nebulous and hard to pin down. A case in point is the evolution of fraudulent fund transfer, or crime coverage. Years ago, crime coverage was provided as part of a separate commercial policy, specifically covering the theft of funds. As social engineering advanced, many more incidents took place where employees were duped into instructing wire transfers based on electronic fraudulent instructions. Insurance coverage adapted too and began offering this as part of some cyber covers several years ago. The challenge has arisen that some reinsurers are not familiar or comfortable with this exposure.

This is an example of how the edges of cyber insurance can blur with other classes of insurance. It is only through careful management of the policy language intent, and the transparency of customer communication and underwriting approach, that the risk can be appropriately managed.

2023 has seen an increase again in the levels of ransomware activity.[11] However, companies are now better prepared, not only preventing the attacks from being successful but also being in a more resilient position if ransomware is deployed. Effective data back-up strategies are more widely used, and companies are more agile in being able to restore data without being held hostage to pay for the decryption keys. It remains an open question as to whether the combination of underwriting actions to manage the potential downside, as well as improved security controls, will limit the translation of increased activity into increased losses in the insurance industry.

Cumulative yearly ransomware revenure, 2022 vs. 2023 (through June)



Source: Chainalysis

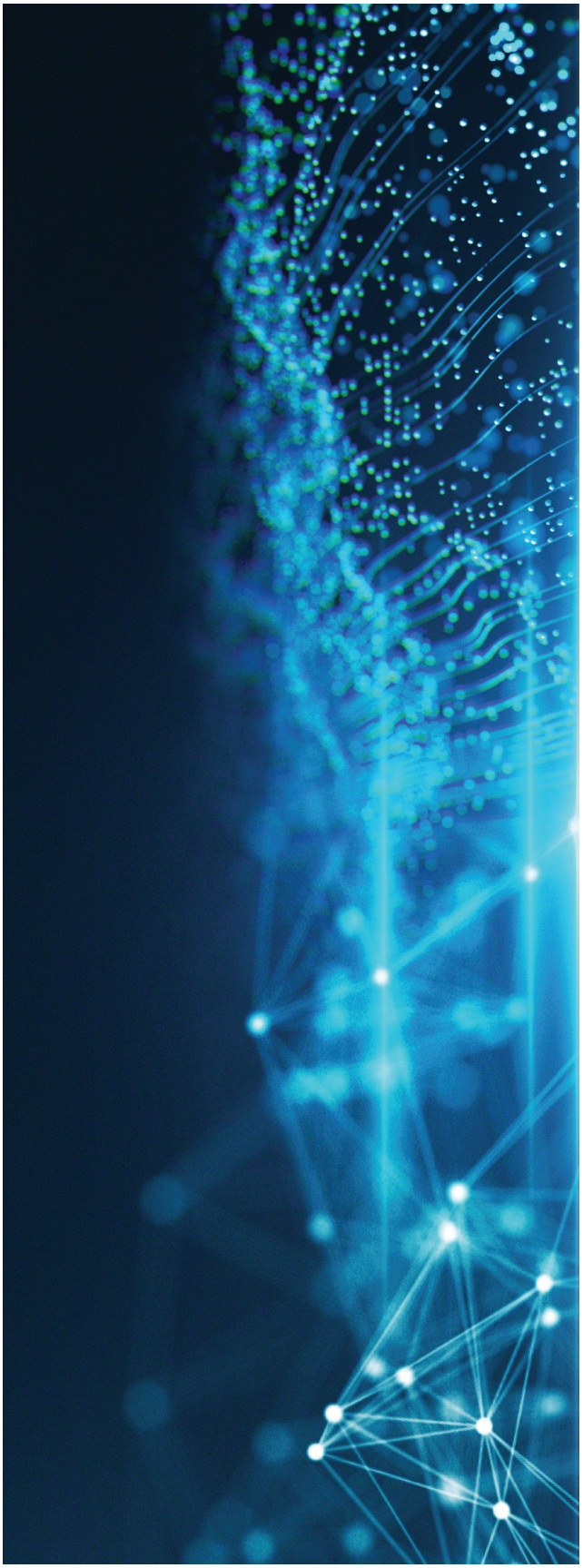
[11]https://blog.chainalysis.com/reports/crypto-crime-midyear-2023-update-ransomware-scams/

> The goal of separating cyber perils into more segregated categories for reinsurers, is to create a better opportunity for varied appetites to support the constituent parts of cyber exposure.

Match making

The goal of separating cyber perils into more segregated categories for reinsurers, is to create a better opportunity for varied appetites to support the constituent parts of cyber exposure. First Party covers with short tail characteristics are more suitable for reinsurers with an appetite for volatility and a desire for a shorter time frame of reserve management. Conversely, those reinsurers who are familiar and comfortable with long tail liability classes of business such as casualty and financial lines, are more likely to gain confidence in the Third Party liability exposures created by cyber risks. These include regulatory issues, consumer and business privacy matters, and potential liability caused by contractual arrangements. Liabilities (especially for those insurers operating in higher excess positions) can take many years to be resolved, and the mindset of managing the reserving process is very different.

Systemic or catastrophic cyber risk created by the inherent interconnectivity between companies and consumers throughout advanced economies, is another distinct type of risk which behaves differently to traditional First and Third Party perils. It requires an approach drawing on the experience of natural catastrophe perils within insurance. The use of exceedance probability curves, modelling, extensive data, and analytics all support the understanding of low frequency, high severity events. These types of peril are well suited for alternative capital markets and can be packaged in a way that is attractive to non-traditional (unrated) capital structures.



How to?

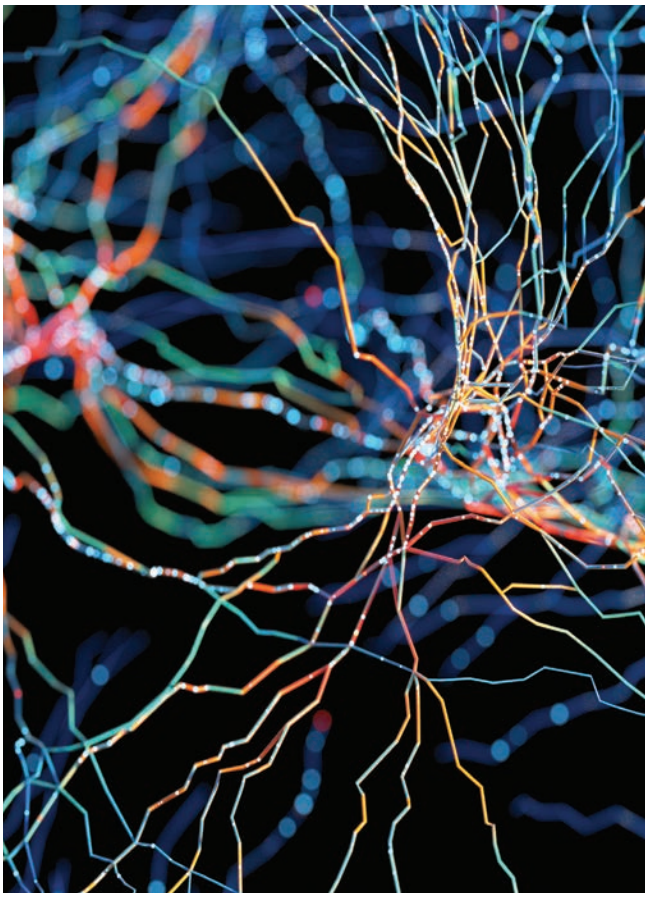
The argument for separating cyber reinsurance into three categories is compelling: First Party perils; Third Party liabilities; and finally and distinctly, systemic cyber risk. Whilst the end buyer of cyber insurance values the combined product, the specialisation within reinsurance enables the separate perils to be treated differently by distinct parts of the market. Even once this approach is accepted in principle and this path makes sense, the challenge remains that there are several obstacles to overcome for the benefits of this approach to be adopted in the market.

> "The specialisation within reinsurance enables the separate perils to be treated differently by distinct parts of the market."

It's all about that data

The most important initial step to streamline risk and capital into improved efficient structures, is to capture risk data in a more accurate manner that is better aligned to separate perils. There needs to be credible and defensible premium allocation, based on underwriting rating between First and Third Party risks. This includes premium for monoline cyber insurance, as well as cyber risks which are part of joint (often E&O) covers, which are harder to track. The accurate capture of claims data is equally critical to demonstrate performance over time for the separate segments of First and Third Party risks, as well as catastrophe risk. Education of both buyers and sellers of cyber reinsurance is an ongoing priority, as the trend to increased specialisation is set to continue. With these steps, much needed reinsurance capacity can support the continued growth of the overall market for years to come.

The Lockton Re Cyber Centre view is that, at least from a reinsurance perspective, the (mostly) "one- size-fits-all" structure of the original product no longer suits an increasingly specialised reinsurance market. We are at a juncture where, as part of the ongoing maturing of the cyber market, qualitatively different coverage deserves qualitatively different treatment by reinsurers and capital providers to maximise the market potential. First Party perils and Third Party liabilities are not the same. Catastrophe losses behave differently from attritional losses. Complex extended legal defence does not compare with the emergency, time-sensitive response required from a forensic expert. These all need a differentiated approach in underwriting, claims and reserving. So, why have they been under one reinsurance umbrella for so long? It takes time to change, but we view this approach can truly create a cyber reinsurance market, which is fit for purpose. As Ralph Waldo Emerson, the nineteenth-century essayist, said: "The shoemaker makes a good shoe because he makes nothing else."



About Lockton Re (locktonre.com)

Lockton Re, the global reinsurance business of Lockton Companies, helps businesses understand, mitigate, and capitalize on risk. With over 350 colleagues in 18 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.

Lockton Re Insights

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 categorize this content in four areas – Perils, Exposures, Risk Transfer and Placement.

Authors:

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

Patrick Bousfield
Lockton Re
Chair, Lockton Cyber Centre
patrick.bousfield@lockton.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

Designed by Rachel Clarke and Anna de Souza Morgan

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

Bermuda
Seon Place, 141 Front Street, 3rd Floor
Hamilton HM19
Bermuda
Office phone number +1 441 294 4864

Zurich
Freigutstrasse 26
8002 Zurich
Switzerland
Office phone number +41 (0) 79 944 84 74

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.

REINSURANCE