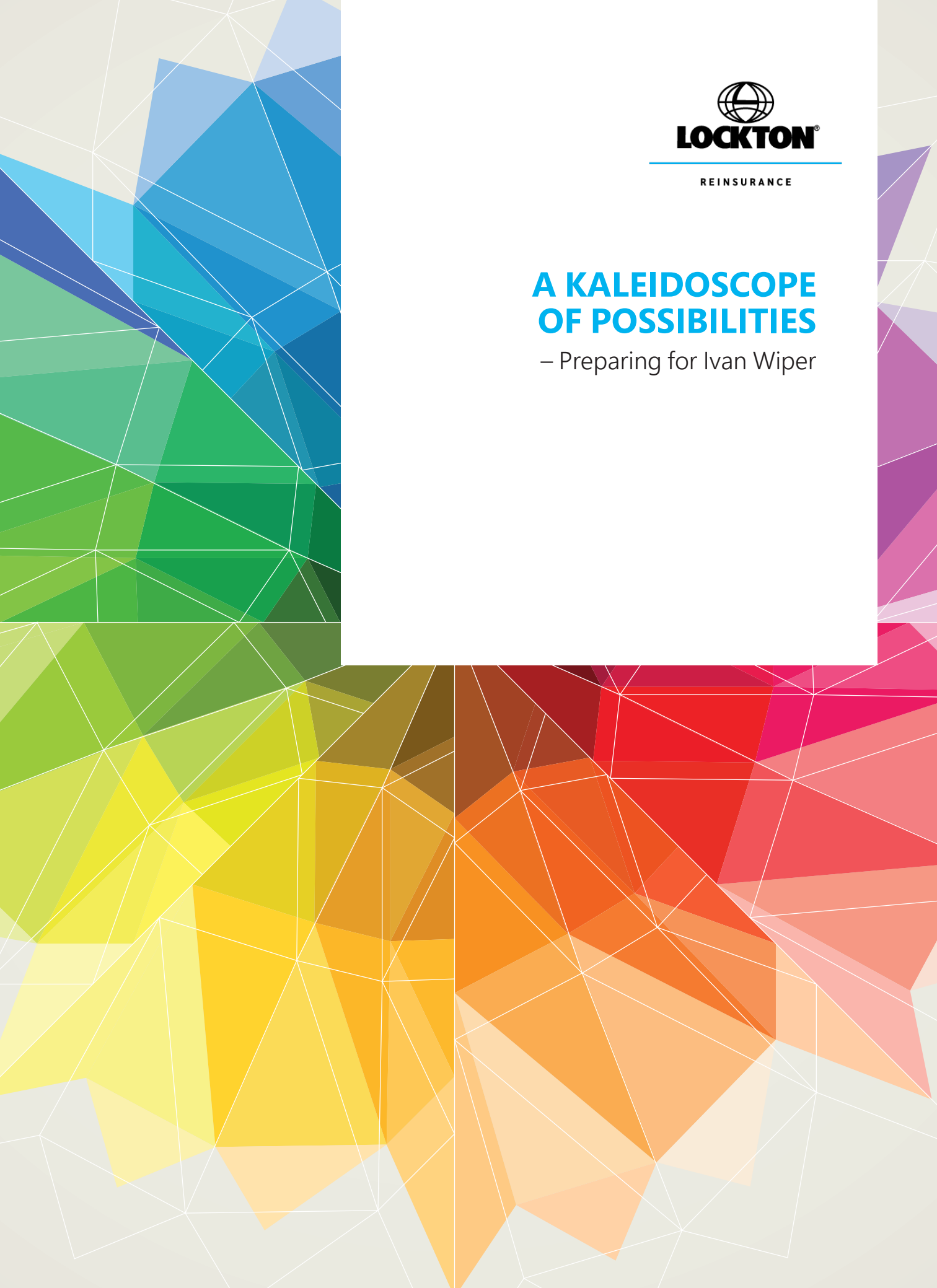
LOCKTON®

REINSURANCE

A KALEIDOSCOPE OF POSSIBILITIES

– Preparing for Ivan Wiper



LOCKTON RE CONSIDER THE GLOBAL IMPACT AND PREPAREDNESS OF THE (RE)INSURANCE INDUSTRY FOR A CYBER CATASTROPHE IN NEW REPORT.

Lockton Re's reports, market commentary and insights focus on key topics, occurrences or changes in the (re)insurance and broking market place that are impacting 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. We interviewed a number of market leaders across the cyber insurance value chain, to bring depth and clarity to our report.

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

Executive summary: the day after Ivan Wiper hits

Cyber catastrophes are the source of much debate within the insurance industry, around their causality, potential frequency, and severity. That debate will continue. However, our goal is to shine a spotlight on the consequences of a potential cyber catastrophe, by focusing on the different parts of the value chain across the insurance industry. What are the short-and long-term impacts? What are the potential unintended consequences? Who are the winners and losers?

We have taken a consensus-based hypothetical catastrophe event type, that of self-propagating destructive malware, (which we've called Ivan Wiper), and assumed a midpoint view of its impact globally. This is the starting point for our assessment.

The goal is to stimulate a considered discussion around planning for cyber catastrophes, and improve understanding and preparedness for such events. To quote one of the great sporting coaches of (American) Football, Vince Lombardi, "Preparedness is the ultimate confidence builder." This is particularly apt in the face of uncertainty in the cyber market. There are several areas where the industry can do more to educate and prepare for a potential cyber catastrophe.

Key takeaways:

1. A scenario such as Ivan Wiper is not existential for the insurance industry. There have been, and will be, bigger natural and man-made disasters in all but the most extreme scenarios.
2. Signs indicate that there will be some benefits to community and incident response at scale.
3. There is unlikely to be sufficient incident response capacity to handle the immediate aftermath of a significant event, and there could be potential major bottlenecks in claims handling and processing.
4. Some (re)insurers may withdraw from the cyber insurance market, though there is strong appetite by those experienced (re)insurers to recapitalise and take advantage of dramatically improved rating conditions. There will be an acceleration of specialist capacity and expertise.
5. A cyber catastrophe could prove a catalyst for product development and a more robust solution set for cyber catastrophe business.

Introduction

The Fourth Industrial Revolution is in full swing – with the internet at its very heart. Network connections are increasing exponentially, and our global neighbourhood is shrinking. Leveraging technology for nefarious intent is not new. But the objectives, strategies and tactics of threat actors are complex and opaque. This context should not immediately spark fear for the insurance industry. The very purpose of our industry is to understand and quantify risk. The management and mitigation of risk has built our industry over centuries, building societal resilience with it. As risk evolves, so too do the solutions, and these include a promise to pay in our customers' hour of need.

Cyber insurance in its current form is an All Risks product[1] which has developed in response to a dynamic and changing risk landscape. One constant however, is the potential for accumulation of systemic risk within a portfolio, and multiple near misses act as a reminder of this. It is incumbent on our industry to address this risk in a grown up, collaborative and articulate manner. It is all too easy to dream up science fiction scenarios; the recent Netflix Original film 'Leave the World Behind' is a case in point. It portrays a post-apocalyptic world in the aftermath of a cyber-attack. The purpose of this paper is not to stir up a frenzy of anxiety about potential disaster scenarios, raising levels of fear, uncertainty and doubt. Our objective is not to debate how an event could manifest, nor what size it could be. The concept of loss aversion is particularly relevant here, as developed by behavioural economists Daniel Kahneman and Amos Tversky in their 1979 paper 'Prospect Theory: An Analysis of Decision under Risk.'[2]

Indeed, Kelly Castriotta, Global Executive Underwriting Officer for cyber, tech and artificial intelligence at Markel commented that "There is a danger that collective imagination and group think, if left unvalidated, could be at best unhelpful and at worst an existential risk to the industry." This observation recognises the need to remove blinkers from our collective thinking and be open to the potential for very unlikely events to upend our conventional approach to the market.

> "There is a danger that collective imagination and group think, if left unvalidated, could be at best unhelpful and at worst an existential risk to the industry."
>
> **Kelly Castriotta, Markel**

The insurance industry has built its reputation by supporting recovery after major events, learning, and adapting. Notwithstanding that a major cyber catastrophe has yet to materialise, the cyber insurance industry has been proactive in addressing the potential for significant systemic risks. Lloyd's and the UK Prudential Regulation Authority (PRA) have pushed for more clarity and confidence in managing downside risk. The much-debated implications of cyber war are important for the industry (and a hornet's nest that will be left alone here). Commercial modelling firms have invested significantly in research and development, and there is an increasing consensus around the types of events that could move the market. The cyber catastrophe model development journey is ongoing, and provides evidence of significant uncertainty in the construction and size of possible events. That is no surprise, given the scale of the challenge.

There has been significant progress in navigating a path through this uncertainty. Uncertainty and risk are the commodities on which the insurance industry is built. Cyber catastrophe risk is a complex but fundamental pillar of the broader market, and insurance carriers set capital against these tail risk metrics. Commercial as well as regulatory scrutiny has increased focus on this risk. At the same time, modelling companies continue to develop their own independent views of this risk. More recently, the capital

[1]Brew, Oliver. 2023. "The All Risk Cyber (ARC) Challenge – an Assessment to Simplify Cyber Reinsurance | Lockton." 2022. Lockton. April 7, 2022. https://global.lockton.com/re/en/news-insights/the-all-risk-cyber-arc-challenge-an-assessment-to-simplify-cyber-reinsurance.
[2]"Prospect Theory: An Analysis of Decision Under Risk on JSTOR." n.d. Www.Jstor.Org. https://www.jstor.org/stable/1914185.

markets and insurance linked security sector are trading in cyber catastrophe bonds on the back of this volatile exposure.

This context provides the objective of this paper. Simply put, the goal is to explore how the cyber insurance market will respond in the aftermath of a major cyber catastrophe event. A major wiperware event, Ivan Wiper, has happened. We know its shape and size. What happens next for the insurance industry? Through a series of interviews with market leaders across the cyber insurance value chain,[3] we have built a picture of how the market likely responds. It provides a macro assessment to overall market resilience, explores potential performance differentiators, and highlights challenges that are not currently given as much attention as they deserve. The aim is to ask questions, challenge assumptions and elevate the level of conversation about what might happen when a cyber catastrophe occurs.

Considering the cyber catastrophe conundrum through an alternative lens is intended as a thought-provoking, mature discussion to support the market as it grows, providing value for customers and opportunities for participants. Building resilience through preparedness is key to the sustainability of the cyber insurance, and wider market.

Setting the scene — the impact of Ivan Wiper

As the starting point for analysis of post-event consequences, a cyber catastrophe is required.[4] Significant economic impact and social disruption is expected. Based on a high-level macro assessment, and market consensus, below are the hypothetical 'facts'.

In-force Global Direct Written Premium: US$20.3bn (projected figure)

Date of Event: November 18th 2026

Event Name: Ivan Wiper

Event Type: Propagating wiperware

Threat Actor: Sophisticated criminal group affiliated with a nation-state[5]

Target System: Very commonly used operating system

Insured Costs: Incident Response, Data Restoration, Customer Notification, Business Interruption, Contingent Business Interruption, Liability

Attritional Impacts: Post event attritional loss deterioration due to claims settlement delays and heightened risk landscape

Global Cyber Market Economics:

- Direct Premium Written: US$20.3bn[6]
- Non-Cat Insured Loss (Loss Ratio): US$11.4bn (56.3% LR)
- Event Insured Loss (Loss Ratio): US$28.4bn (140.0% LR)
- Industry Annual Loss (Loss Ratio): US$39.8bn (196.3% LR)

[3]See Acknowledgements for participants on Page 18
[4]The cyber catastrophe is based on the consensus of cyber catastrophe models CyberCube and RMS, both of which state that destructive malware is most likely to lead to widespread economic impact. "CyberCube – Cyber Insurance Analytics – Managed Cyber Insurance Risk." n.d. "Catastrophe Models and Risks." n.d. https://www.rms.com/models.
[5]Although the criminal group has connections to a nation-state, there is insufficient evidence to meet the threshold definition of an act of war in any contemporary cyber insurance policies
[6]Lockton Re estimate of US$13bn Global Cyber Direct Written Premium at the end of 2023, with 16% forecasted annual growth (rate change and new business) projected forward to end of 2026

Exploring how the insurance industry has reacted in the past

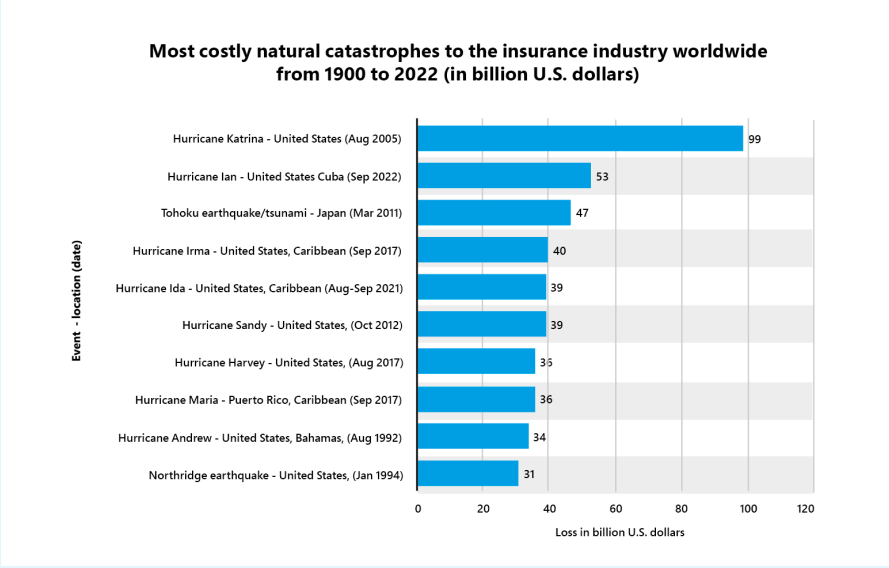


Figure 1 "Largest Insurance Losses in History 1900-2022 | Statista," August 22, 2023. https://www.statista.com/statistics/267210/natural-disaster-damage-totals-worldwide-since-1970/

There have been many landmark natural and man-made catastrophes that, in addition to causing human suffering, have been milestones for the development of the insurance industry. Here are some examples of the aftermath of such catastrophes.

1992 Hurricane Andrew

Hurricane Andrew hit in August 1992 and was at the time was one of the biggest economic and insurance losses in history.[7] Apart from the tragic loss of life and property, there were significant implications for the property catastrophe insurance industry. The rudimentary assessments of the potential coastal damage dramatically underestimated the impact of the hurricane. There were multiple insurance company insolvencies, and legislators intervened in the ability for insurers to change rates or withdraw from the market. There was a major market failure in the immediate aftermath, and a larger role for government was required to make insurance available for those with property close to the coast.

Reinsurance[8] became more widely used to share the risk outside the region, as well as the nascent development of insurance linked securities, enabling investors to participate in trading the risk as an alternative asset class. Computational modelling for catastrophe risk developed, as well as improvements to building codes, and other mitigation steps designed to help people better withstand the impact of a hurricane.

- **Insured Loss Estimate: US$34bn (2022 dollars)**
- **Insurer Insolvencies: 11[9]**

[7] McChristian, Lynne and Insurance Information Institute. 2012. "HURRICANE ANDREW AND INSURANCE: THE ENDURING IMPACT OF AN HISTORIC STORM." https://www.iii.org/sites/default/files/paper_HurricaneAndrew_final.pdf.
[8] Ibid
[9] Ibid

2011 Tohoku earthquake

In March 2011, the most powerful earthquake ever recorded at 9.1 on the Richter scale, caused a massive tsunami wave over 40 metres high to devastate eastern Japan. There were close to 20,000 fatalities and three reactors in the Fukushima nuclear power plant were destroyed.[10] The tsunami was larger than any expectations and led to improved understanding of secondary loss factors. Liquefaction[11] and contingent business interruption were significant contributors to loss.

- **Insured Loss Estimate: US$35bn[12] (2022 dollars)**

Terrorist attacks, September 11th 2001

The terrorist attacks on New York and Washington are well-documented and caused horrendous loss of life and property. From an insurance perspective, they reshaped the industry, given the scale of the losses. Prior to 9/11, terrorism was not underwritten, charged for, or excluded in most commercial property insurance. Additionally, the US Congress established the Terrorism Risk Insurance Act, providing a backstop for the industry, to maintain coverage at affordable rates.

- **Insured Loss Estimate: US$40bn[13] (2022 dollars)**

Exploring the value chain

Our research engaged stakeholders across the insurance value chain. Investors and capital markets are at one end, running through intermediaries and (re)insurers to the ultimate policy holder at the other end. We investigated the short- and long-term consequences Ivan Wiper would have on different aspects of the insurance industry, claims handling, longer term viability, and existential concerns.

[10]BBC News. 2023. "Fukushima Disaster: What Happened at the Nuclear Plant?" BBC News, August 23, 2023. https://www.bbc.co.uk/news/world-asia-56252695.
[11]"Liquefaction With the Great East Japan Earthquake." 2018. In Elsevier eBooks, 147–59. https://doi.org/10.1016/b978-0-12-814078-9.00008-x.
[12]"Williams, Chesley. "A Look Back at the 2011 Great East Japan (Tohoku) Earthquake | Moody's RMS." 2021. March 10, 2021. https://www.rms.com/ blog/2021/03/10/a-lookback-at-the-2011-great-east-japan-tohoku-earthquake.
[13]Davis, Marc. 2023. "The Impact of 9/11 on Business." Investopedia. September 11, 2023. https://www.investopedia.com/financial-edge/0911/the-impact-of-september-11-on-business.aspx#toc-business-takes-a-hit.

> When taking the bird's eye view, order is maintained. The insurance industry will brush it off.

The bird's eye view – keep calm and carry on

When the dust settles following Ivan Wiper, the insurance industry experiences a US$28.4bn event loss. It is certainly a capital impacting shock, but not in any way existential. This is not unusual in the (re)insurance world, and there is a demonstrable history of the industry bouncing back from this type of catastrophe. Using a global non-life insurance premium estimate of US$4.9tn,[14] it is only a 0.6% shock on the global non-life loss ratio. An event of this size would put it just outside the Top 10 list of most costly events the industry has ever absorbed.

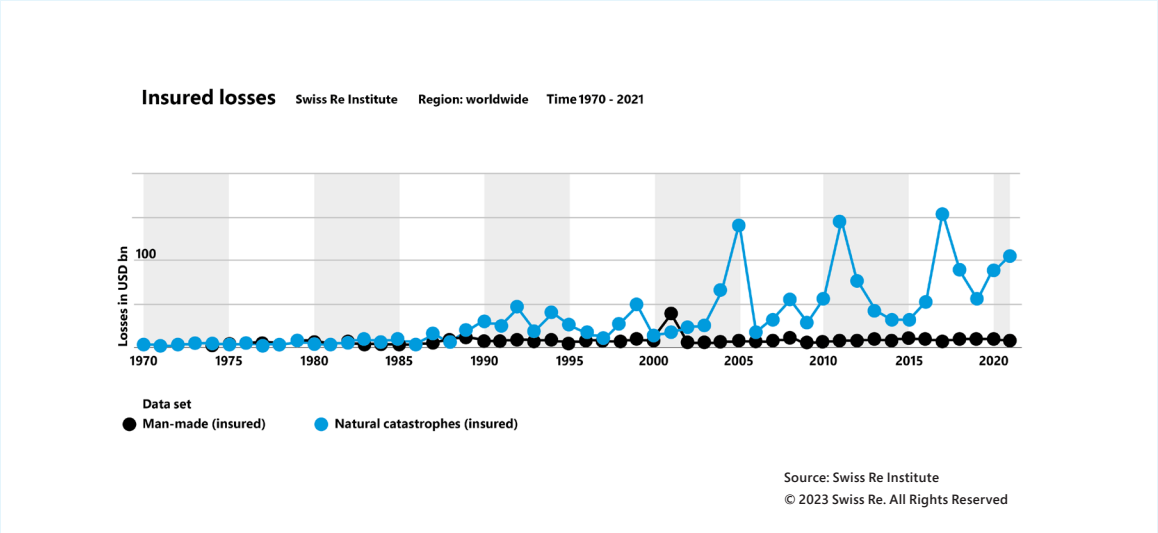
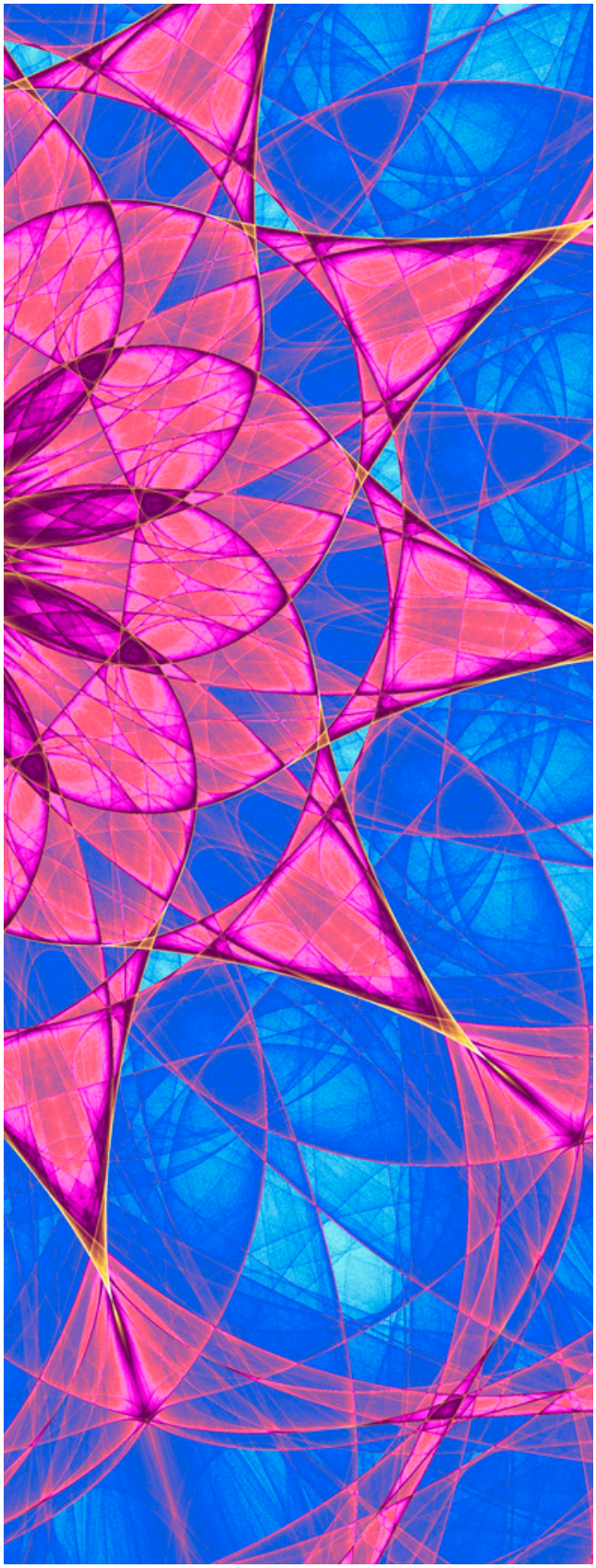


Figure 2 Swiss Re Institute https://www.sigma-explorer.com/

When taking the bird's eye view, order is maintained. The insurance industry will brush it off. This is important context to mitigate the understandable concerns around the uncertainty of cyber catastrophes. There will however be winners and losers, and some parts of the value chain will have transformational changes. Our research and interviews make clear that some elements of our existing cyber insurance market will be tested in the extreme. With a clearer sight of the potential impacts, we can better prepare.

[14]"Sigma Research | Swiss Re." 2024. Sigma Research | Swiss Re. April 15, 2024. https://www.swissre.com/institute/research/sigma-research.html. Based on Swiss Re Sigma estimate of 2022 Global non-life premium of US$4tn, trended with a projected 5.3% annual growth rate to 2026



One level down: the cyber insurance market

The global P&C insurance industry will carry on and shrug off the event. However, for participants in the rapidly growing cyber insurance market, there will be significant implications.

On a premium base of US$20.3bn, the global cyber insurance industry event loss ratio is 140.0%. One consequence is that a cyber shock loss of this nature will cause additional deterioration in the attritional loss ratio for the year. Assuming a 25% deterioration on an average portfolio mean loss ratio of 45%, this leads to 56.3%. Taking both catastrophe and attritional losses into account, this equates to a global cyber insurance industry aggregate gross loss ratio result of 196.3% for the year. We will explore each segment of the cyber insurance value chain in turn, so as to examine the impacts.

> "The exposure to cyber is a drop in the bucket compared to Florida wind."
>
> **ILS investor**

Capital markets

The investor markets, including insurance linked securities, currently have the least skin in the game. Approximately US$500mn is exposed today, so by the time of the Ivan Wiper attack, this could grow three-fold to an estimated US$1.5bn. This compares with over US$100bn invested in natural catastrophe bonds. As one ILS investor said, "The exposure to cyber is a drop in the bucket compared to Florida wind." Contracts are mainly focused on cyber catastrophe bonds for low frequency, high severity events, attaching only in extreme events. Convincing investors to deploy capital has involved a lengthy process of education. Throughout, understanding a sponsor's underwriting process, governance and standards has been critical. Of equal importance has been the analysis and understanding

of how an event would manifest compared to expectations. This will determine the Capital Market response post event. Capital Market trading relies heavily on an independent, modelled view of risk. Therefore, the efficacy of models are core to the long-term success of this market. "The largest question for the capital markets is when the event happens, does it happen in an expected way?" said Brittany Baker, VP of Solution Consulting at CyberCube.

Given the scale of the Ivan Wiper event, capital will be locked up from day one, so it is fair to assume a total loss. Key questions include those at both individual company level and at industry level.

- What happened?
- Why did it happen?
- What are the impacts?
- How did the event compare with modelled outputs?
- Are there any blind spots in the model scenarios?

Ivan Wiper is broadly within expectations. This will be a key learning point and provide additional confidence in the models and ILS structures being traded. Those funds which have been building an understanding over time through 'dipping the toe in' will be best placed to leverage the market dislocation. "We'll lean in to take advantage of extended attractive conditions," said another investor. There have been prior examples where this hasn't been the case, such as in the aftermath of some wildfires which caused outsized losses for issuers of cat bonds.

"A distressed segment plays into the hands of alternative capital," according to one ILS investor. Lead investors will be able to recapitalise the market with rates above natural-catastrophe bonds. (Re)insurers who demonstrate differentiated underwriting and exposure management experience will be favoured. Funds with de minimus participation have built the confidence in the asset class and will maximise returns by pivoting capital to support the distressed class. Funds who were watching from the outside waiting for the event, use this as a chance to follow on the coattails of the pioneers to benefit from the significant rate rises.

Rated reinsurance capacity

An estimated 55%[15] of all direct premiums written are reinsured within the cyber market. That is materially higher than other more mature lines of business. Proportional reinsurance makes up most of the limit reinsured with different forms of non-proportional limit being purchased to top up coverage. Typical market terms for most current cyber reinsurance products provide the context for considering the impact on the cyber market.

- **Quota Share — The historical core pillar of Cyber treaty purchasing. Loss ratio caps continue to be commonplace in most treaties limiting recoveries.**
- **Aggregate Stop Loss — Commonly attaching in the 125%-175% range on a gross basis. Limits purchased vary by cedant depending on a multitude of factors, for example other reinsurances purchased, price, risk tolerance, etc. The limit stretch purchased tends to be driven by a net risk appetite position to meet management risk tolerances.**
- **Occurrence Excess of Loss —There is undoubtedly a trend towards exploring, and more recently converting, event purchases with both rated and collateralised markets. The buying intent is to purchase coverage that responds to an event, excluding attritional loss. It typically attaches at a lower gross loss ratio to reflect this.**

[15]"Global Cyber Insurance: Reinsurance Remains Key to Growth." n.d. S&P Global Ratings. https://www.spglobal.com/ratings/en/research/articles/230829-global-cyber-insurance-reinsurance-remains-key-to-growth-12813411.

The current marketplace enables reinsurers to limit downside risk for cyber. Simplistically, reinsurers define the amount of capital available to support cyber risk and manage aggregate limit deployed tightly against this number. Given the losses faced after Ivan Wiper and typical terms achieved in the common reinsurance trades, it is fair to assume that most reinsurance capital allocated to cyber risk has been eroded.

No doubt a suffering reinsurance market will be re-capitalised, given that capital flows to distressed markets. Some reinsurers will no doubt pull out of the class altogether. The more prepared participants will see this as an opportunity to take advantage of the situation. Reinsurance rates will spike to recoup losses providing those comfortable to redeploy with healthy returns in upcoming renewals.

According to one reinsurance buyer, an interesting consideration will be the timing of the event. The interaction between the timing, speed and scale of the rate increase hitting the direct market will flow through the reinsurance market in different ways. This will depend on inception date, treaty basis, fixed limits versus limits variable on premium, etc. Those reinsurers which plan for a catastrophe such as Ivan will likely fare better.

History of profitable reinsurance writing – those with a longer history of writing the class profitably will be better prepared to absorb losses from an event, through articulation of this as part of a long-term investment cycle. It would also likely be easier to convince investors of the potential for future good years ahead.

Scale of portfolio – those reinsurers who have a large enough portfolio, which is more diversified by sector, size and geography, will most likely have below market share impacts. They will also be better placed to access higher level market intelligence to leverage the market position in the aftermath of Ivan.

Awareness of risk and volatility – being ready for the event will ensure that senior management and capital providers are not left surprised by it. Those boards who understand that Ivan losses are within expectation will be most ready to pull the trigger to recapitalise.

Team expertise – those with teams that are better educated will give senior management more comfort and confidence in redeploying capital. Having the expertise to identify successful portfolios and ensure the deals are structured in the right way, will be critical to making senior management feel comfortable to redeploy.

Future underwriting controls – Research into cyber catastrophe management will be a focus and the factors driving the relative performance will filter into the underwriting process of catastrophe exposed treaties. There may be underwriting conditions specific to Ivan that separate reinsurers from each other, based on their performance.

Product development – there will be a forensic review of the performance of the reinsurance products currently available. It is likely that more focus will be placed on developing products to create covers split attritional loss from systemic loss. Although this development is already in flow, there is significant underinvestment in truly understanding event covers from a technical perspective. More resource will be invested in the topic to supercharge the development of the cyber catastrophe market.

Direct insurance writers

Moving one step along the capital chain, let's turn to direct underwriters of cyber risk. After Ivan Wiper, they will certainly be feeling the heat. Reinsurers and capital markets will be writing off their limited capital deployed and implementing strategies for reinvesting, given the opportunity. However, direct writers will be in the lion's den; in the detail doing what the cyber insurance industry is there to do. One priority is to avoid an outsized loss, compared to market share. They will be supporting clients to respond and recover from thousands of claims through incident response, claims adjustment and settlement.

The macro level impact on the average insurer will be manageable. Reinsurance capacity is eroded, but the event is not significant enough for all reinsurance limits to be hit. Insurance capital has been set to absorb this event, and the long term viability of most insurers is not at risk. For those who have well thought out and clearly articulated views of risk and appropriate risk tolerances in place, the ultimate result should not be a surprise. Undoubtedly, however, some direct writers will fare better than others.

Portfolio management – Insurance 101 – writers that have constructed 'optimal' portfolios will come out of the event looking good versus their peers. The direct cyber market has a history of being quick to adapt. The actual benefits of the diversification presented to date will be tested. As Michelle Faylo, US Cyber and Technology Practice Leader of Lockton insurance brokers said, "those insurers that focus on core risk controls and have built a balanced, diversified portfolio will experience differentiated results".

> "Those insurers that focus on core risk controls and have built a balanced, diversified portfolio will experience differentiated results."
>
> **Michelle Faylo, Lockton**

Coverage offered – Underlying coverage provided will also be a driver of results by carrier. As Ivan Wiper unfolds, it becomes clear that there is collateral damage, i.e. companies impacted because of a digital link to a directly impacted organisation. The level and criticality of reliance and dependency on these connections is notoriously difficult to track in the cyber modelling world, but will be material to the ultimate loss.

Coverage will vary (for example, including voluntary shut down costs) and this will influence the final losses. Contingent Business Interruption, which extends cover to companies upon which the insured is reliant, is relatively common, especially for larger companies. This will increase losses, though sublimits will be important. System Failure coverage, which does not require a malicious attack to trigger cover, will be settled more quickly as there is a lower threshold for evidence of loss. The level of granularity in data capture for sublimits will impact this as well. Insurers who have been actively managing coverage to a systemic event will have higher certainty on total exposed limits more quickly and accurately than peers. This could be tracking disaster scenario models or using technology data to understand connections and key areas of potential concentration risk. There are many studies on this topic.[16] The nature of critical infrastructure and war exclusions across portfolios will all drive variance in carrier results. The conclusions of these will obviously only come to fruition after an elongated and uncertain process in the courts.

Insurance claims response – the claims response is where the rubber hits the road. Historical natural catastrophe examples provide lessons on how the industry might respond to a cyber event. Putting the policyholder first will be of utmost importance, after all this is exactly what the industry is here to do: provide support in the hour of need. Some insurers have established retainers with major incident response providers to secure capacity when Ivan Wiper arrives. This also highlights major differences between the cyber and physical worlds. This event is not bound in the same way by geography. How effectively an insurer can mobilise its claims response will be a huge driver of differentiation in both results and reputation.

With the backdrop set, it's clear that there will be significant differentiation in results. As the dust settles, senior management will have to consider how to bounce back. Maintain the status quo? "We knew what we were doing, we were doing it well and we saw this event coming." Pull out? "We didn't get that right, we're hurting, and we're scared." Lean in? "We've been waiting for this. We're comfortable with the risk and have the infrastructure in place to benefit from these rates".

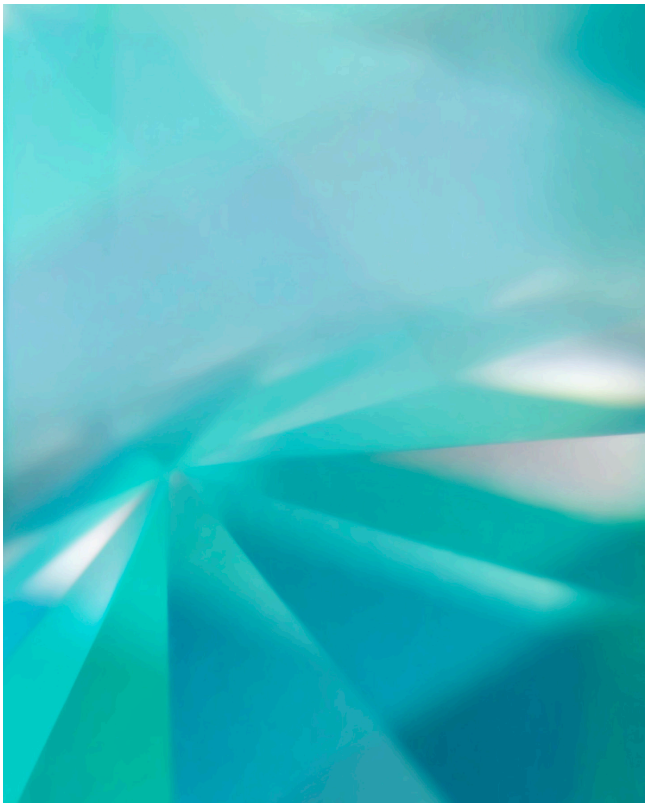
[16]European Systemic Risk Board. 2020. "Systemic Cyber Risk." Systemic Cyber Risk. https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.
[17]Davies, Nahla. 2024. "The Evolving Role of Cyber Insurance in Mitigating Ransomware Attacks." Secureworld (blog). March 20, 2024. https://www.secureworld.io/industry-news/role-cyber-insurance-mitigating-ransomware.

> There will be a flight to quality, and those carriers with experience and credibility will be beneficiaries.
>
> **Max Perkins, Spektrum Labs**

How long a carrier has been in the space, and whether they have the historical profitability to support a spike in the loss ratio, will certainly be factors. So too will be the people, processes, and product in place. Those that have invested, with more established teams and deeper expertise, will not be surprised by the event which had been articulated internally. Senior management will be more comfortable that the team can navigate the uncertainty and come out the other side stronger. As Max Perkins of Spektrum Labs said, "There will be a flight to quality, and those carriers with experience and credibility will be beneficiaries." As the market emerges from Ivan Wiper, it is clear that there will be seismic changes. We've seen from historical catastrophes, both natural and man-made, that previously unseen shock events can shape a market. Ivan is no different. However, given the work already done by the cyber insurance market to get ahead of the risk, these changes are likely to be less dramatic than other classes.

Rates increases – rates will hike. They always do. Although systemic price loads are considered for cyber insurance, the fall-out from Ivan will call into question whether it was enough. Whilst that analytical work takes time, the insurance buying community has not been able to get away from day to day media coverage of the event, and whether directly impacted or not, risk perception will be at its highest level. Increases in premiums will be driven through and accepted by buyers.

Penetration rate – that heightened risk perception will also drive increased penetration rates. Historically



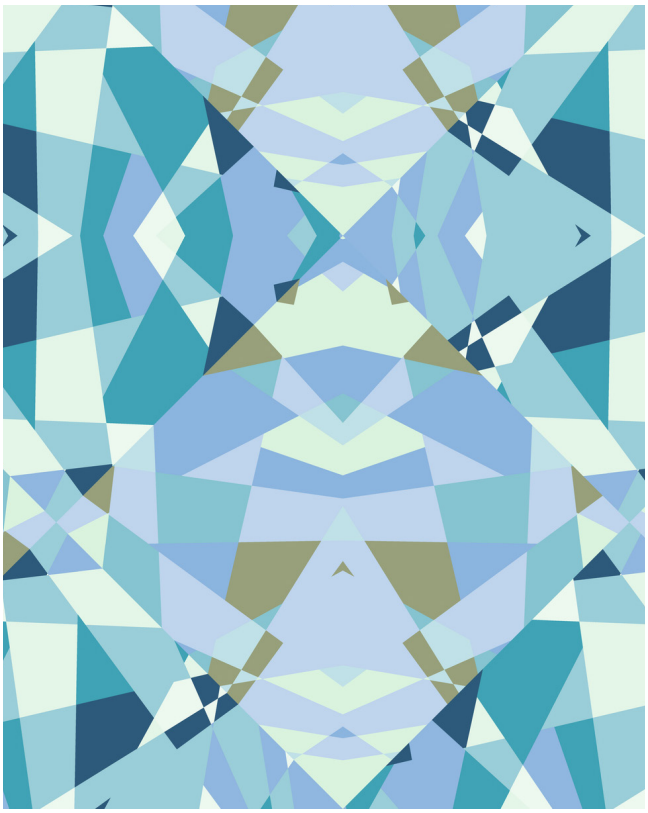
underpenetrated markets like small and medium businesses, as well as emerging markets get the catalyst they need to fast track growth. Even in mature markets, there are still many companies that do not buy cyber insurance. There will be a dramatic increase in demand, though now at elevated prices, creating a once-in-a-generation opportunity.

Portfolio management improvements – it will take time to conclude, but deep dive reviews into where losses come from across individual portfolios will show patterns. Learnings will be taken from how losses spread across company size, geography, and industry. Specific work on analysis of the impact of risk controls on losses[17] (e.g. backups, application of MFA) will provide valuable portfolio insights. This will be a true test of the existence of diversification in the line of business. Those with the differentiated data availability and expertise in place will be able to draw more insightful conclusions, more quickly than peers. This leads to more active and refined portfolio management which better considers the systemic nature of the risk.

> We have a habit of underwriting using the rear view mirror, instead of what's in front of us.
>
> **Daniel Carr, Ariel Re**

Coverage development – As insurers unpick the impacts, front and centre of the discussion will be how the market should address systemic risk in the future. With a tangible cyber catastrophe no longer hypothetical for buyers and sellers, consideration must be given to whether a cyber catastrophe insurance market develops. There are market players that have already moved in this direction, and being proactive is refreshing in an industry which has often been reactive. As Daniel Carr, Head of Cyber at Ariel Re said, "We have a habit of underwriting using the rear view mirror, instead of what's in front of us." But Ivan Wiper turbocharges the market into shifting into a bifurcated attritional (standard) and catastrophe market. Ultimately, this should benefit all through targeting capital more efficiently towards the risk that it wants to take. Although some markets may consider it unfair to restrict coverage for the buyer post the event, ultimately the magnitude of the event is the catalyst for the shift.

Event post-mortem and model development – from Day One the event will be dissected and analysed, then re-dissected and re-analysed some more. Model vendors will look to get their arms around loss estimates. Industry bodies such as Cyber Acuview[18] provide another validation point. In the UK, the Cyber Monitoring Centre[19] has recently been established as a fledgling operation to assess and monitor the severity of cyber events that impact UK companies, which is a welcome initiative. At a high level, the question will be ''was the event within the modelled event set?'' This will differ by model vendor but will be an important item for the market to consider. Each facet of the event will be compared to models, such as the contagion, footprint, number of type of companies impacted. Other areas for investigation include which controls were effective (if any), and how this impacted the loss at a company level. Investment will be made in back-testing the models, a core part of model validation that has been limited in the cyber insurance industry. This serves as a positive step to reduce the overall uncertainty within the market.



Boots on the ground: incident response

Notwithstanding differentiation in individual insurer performance, the market will manage the loss, learn, and rebound stronger and more knowledgeable. At this point, it is necessary to highlight the people whose shoulders this corollary relies upon. For our view to hold, the role of claims adjustors and incident responders is critical and currently untested.

[18] "CyberAcuView". 2021. CyberAcuView. June 4, 2021. https://cyberacuview.com/.
[19] "CMC – Cyber Monitoring Centre." n.d. https://cybermonitoringcentre.com/.

Demand surge is often debated in the cyber market. There is evidence of loss amplification through demand surge in the natural catastrophe world and it has not been tested in cyber insurance. There is a school of thought that solutions to problems in the digital world can be scaled efficiently and effectively. And there are examples[20] of this scalability of response reducing overall loss in past events. In addition, community response[21] is real in the cyber security world. During the WannaCry ransomware attack, a security researcher identified a 'kill switch' which mitigated its impacts.[22] Identification of a vulnerability and corresponding fix will happen efficiently. This can be rolled out at scale, and incident responder playbooks enable a repeatable process. Whilst this version of reality may hold true, the 'anti-demand surge' argument is not proven on an event which has the scale and complexity as the Ivan Wiper.

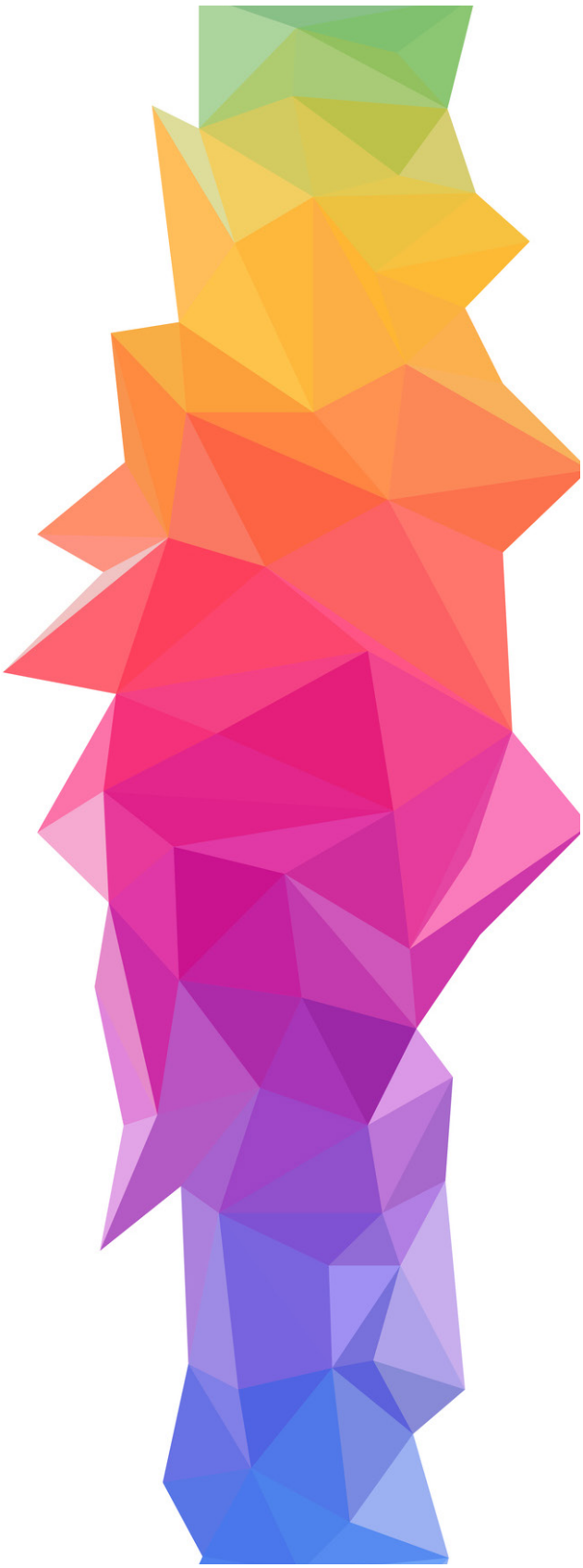
One incident response provider highlights the differentiation between mature insurers where catastrophe planning is more developed, and those who may struggle to secure access to responders following Ivan Wiper. Additionally, the insurance claims process still only has finite capacity. The claims process is complex and requires prescribed workflows that cannot be ignored; claims handlers will need to answer the phone, scope out individual claims, navigate the nuances of contractual obligations and manage stretched vendor panels. Some more mature players have in-house incident responders, and there is a strong case to say these will be more prepared and fare better after a catastrophe event. Incident responders will have similar issues navigating communication lines that are red hot. Priority will be given to clients who are part of critical infrastructure, e.g. utilities, healthcare, food suppliers. Insurance clients with deeper relationships, who have run scenario planning with the claims supply chain, and who have contractual commitments for surge capacity will be serviced next.

> Running through a 'catastrophe play book' with insurer partners helps develop a common understanding of the key factors in setting up for success when it matters.
>
> **Jennifer Coughlin, Mullen Coughlin**

The depth of bench strength in the claims and incident response space is a serious concern. Jennifer Coughlin, Partner at Mullen Coughlin, a breach response law firm, stated that "Running through a 'catastrophe play book' with insurer partners helps develop a common understanding of the key factors in setting up for success when it matters". Ivan Wiper could have the potential to overwhelm claims teams. Events like MoveIt,[23] BlackBaud[24] and Kaseya[25] have encouraged the formation of cyber catastrophe management plans and provided simple validation of the theory, but the sheer number of matters seen has not yet pushed the ecosystem to its limits. Just a few additional matters coming in over a few weeks following Ivan Wiper would stretch the industry claims machine.

These are real concerns, but the positive takeaway is that they are being considered along the value chain by leaders across the market. Digesting lessons from the natural catastrophe response process, engaging with incident response panels, training internally for cross class staff to assist in the hour of need, should all be core aspects of a catastrophe management plan that is actively updated, effectively socialised, and conceptually tested.

[20] Shi, Catrin. 2021. "CFC: Real-life Systemic Cyber Events Challenging Model Assumptions | Insurance Insider." Insurance Insider. December 29, 2021. https://www.insuranceinsider.com/article/29eg3lhzopfx8r3rvr2f4/cfc-real-life-systemic-cyber-events-challenging-model-assumptions.
[21] "'Accidental' Hero Who Helped Slow Cyber-attack." 2017. https://www.bbc.co.uk/news/av/technology-39907055.
[22] Newman, Lily Hay. 2017. "The WannaCry Ransomware 'Kill Switch' That Saved Untold PCs From Harm." WIRED, May 13, 2017. https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/.
[23] "MOVEit Vulnerability and Data Extortion Incident." n.d. https://www.ncsc.gov.uk/information/moveit-vulnerability.
[24] Kelion, By Joe Tidy & Leo. 2020. "Blackbaud Hack: Universities Lose Data to Ransomware Attack." BBC News, July 23, 2020. https://www.bbc.co.uk/news/technology-53516413.
[25] Zach Whittaker. "Kaseya hack floods hundreds of companies with ransomware" TechCrunch Is Part of the Yahoo Family of Brands." 2021. July 5, 2021. https://techcrunch.com/2021/07/05/kaseya-hack-flood-ransomware/.TechCrunch Is Part of the Yahoo Family of Brands." 2021. July 5, 2021. https://techcrunch.com/2021/07/05/kaseya-hack-flood-ransomware/.



Conclusion

The consequences of Ivan Wiper are felt far beyond the insurance industry stakeholders reviewed here. There are many other considerations outside the scope of this paper, in particular, the impact on society and the uninsured. The role of the government could be critical, both in supporting an initial emergency response, and potentially providing financial support in some form to those affected. Indeed, as a recent example, the role of governments in providing financial assistance during the Covid pandemic, was very substantial indeed.

For the insurance industry itself, our view is that the most likely effect of Ivan Wiper will be the acceleration of a cyber catastrophe market with new product innovation, and a growing consensus around common cyber war and critical infrastructure exclusions. For those companies who either cannot afford, or choose not to buy insurance, the impact could be significant. They will struggle to access specialist incident response services unless they have in-house or retained access. Resilience to whatever third party dependencies exist will be tested in the extreme, and there may be insolvencies as a result.

The goal of this paper is to raise questions and challenges, rather than fear or anxiety. By considering specific issues for each stakeholder, the conversation can progress. Training the collective response muscle in preparation for a cyber catastrophe builds resilience for the insurance industry, as well as raising awareness of the risks for society at large.

Acknowledgements

Lockton Re acknowledges and appreciates the following contributors for their thoughtful input in providing a range of perspectives for this paper. In addition to the names below, there are several contributors who prefer to remain anonymous, whom we would like to thank.

Kelly Castriotta, Markel

Matthew Northedge, Canopius

Jennifer Coughlin, Mullen Coughlin

Tom Draper, Coalition

Daniel Carr, Ariel Re

Damini Mago, RMS

Brittany Baker, CyberCube

Deborah Hirschorn, Lockton Companies

Michelle Faylo, Lockton Companies

Max Perkins, Spektrum Labs

Joanna Syroka, Fermat Capital Management

About Lockton Re (locktonre.com)

Lockton Re, the reinsurance business of Lockton, helps businesses understand, mitigate, and capitalize on risk. With over 400 colleagues in 17 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

Matthew Silley
Lockton Re London
Broker
matthew.silley@lockton.com

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

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

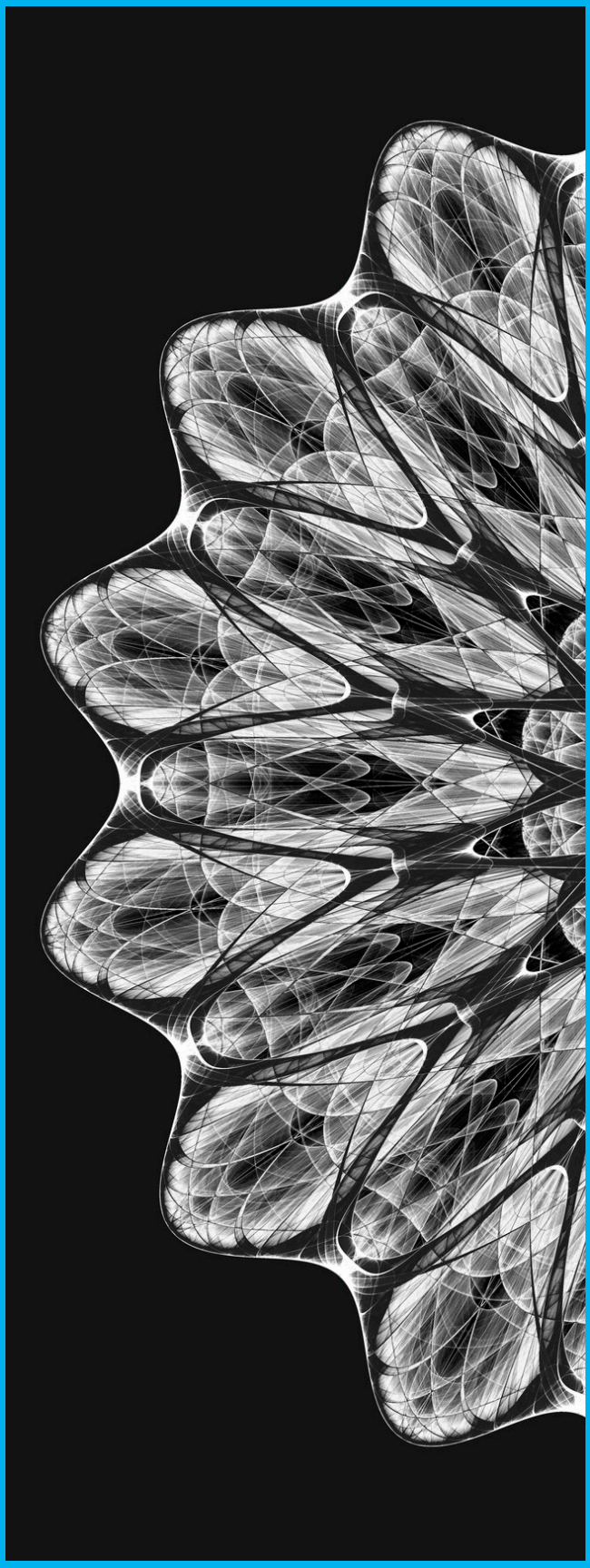
Addresses:

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

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

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



Sources

BBC News. "'Accidental' Hero Who Helped Slow Cyber-attack." 2017. https://www.bbc.co.uk/news/av/technology-39907055.

BBC News. 2023. "Fukushima Disaster: What Happened at the Nuclear Plant?" BBC News, August 23, 2023. https://www.bbc.co.uk/news/world-asia-56252695.

Brew, Oliver. 2023. "The All Risk Cyber (ARC) Challenge – an Assessment to Simplify Cyber Reinsurance | Lockton." 2022. Lockton. April 7, 2022. https://global.lockton.com/re/en/news-insights/the-all-risk-cyber-arc-challenge-an-assessment-to-simplify-cyber-reinsurance.

"Catastrophe Models and Risks." n.d. https://www.rms.com/models.

"CMC – Cyber Monitoring Centre." n.d. https://cybermonitoringcentre.com/.

"CyberAcuView". 2021. CyberAcuView. June 4, 2021. https://cyberacuview.com/.

"CyberCube – Cyber Insurance Analytics – Managed Cyber Insurance Risk." n.d. https://www.cybcube. com/

Davies, Nahla. 2024. "The Evolving Role of Cyber Insurance in Mitigating Ransomware Attacks." Secureworld (blog). March 20, 2024. https://www.secureworld.io/industry-news/role-cyber-insurance-mitigating-ransomware.

Davis, Marc. 2023. "The Impact of 9/11 on Business." Investopedia. September 11, 2023. https://www.investopedia.com/financial-edge/0911/the-impact-of-september-11-on-business.aspx

European Systemic Risk Board. 2020. "Systemic Cyber Risk." Systemic Cyber Risk. https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

"Global Cyber Insurance: Reinsurance Remains Key to Growth." n.d. S&P Global Ratings. https://www.spglobal.com/ratings/en/research/articles/230829-global-cyber-insurance-reinsurance-remains-key-to-growth-12813411.

Kelion, By Joe Tidy & Leo. 2020. "Blackbaud Hack: Universities Lose Data to Ransomware Attack." BBC News, July 23, 2020. https://www.bbc.co.uk/news/technology-53516413.

"Largest Insurance Losses in History 1900-2022 | Statista." 2023. Statista. August 22, 2023. https://www.statista.com/statistics/267210/natural-disaster-damage-totals-worldwide-since-1970/

"Liquefaction With the Great East Japan Earthquake." 2018. In Elsevier eBooks, 147–59. https://doi.org/10.1016/b978-0-12-814078-9.00008-x.

McChristian, Lynne and Insurance Information Institute. 2012. "HURRICANE ANDREW AND INSURANCE: THE ENDURING IMPACT OF AN HISTORIC STORM." https://www.iii.org/sites/default/files/paper_HurricaneAndrew_final.pdf.

"MOVEit Vulnerability and Data Extortion Incident." n.d. https://www.ncsc.gov.uk/information/moveit-vulnerability.

Newman, Lily Hay. 2017. "The WannaCry Ransomware 'Kill Switch' That Saved Untold PCs From Harm." WIRED, May 13, 2017. https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/.

"Prospect Theory: An Analysis of Decision Under Risk on JSTOR." n.d. Www.Jstor.Org. https://www.jstor.org/stable/1914185.

Rudden, Jennifer. "Most costly disasters to the insurance industry worldwide 1900-2022" Statista. August 22, 2023. https://www.statista.com/statistics/267210/natural-disaster-damage-totals-worldwide-since-1970/

"Sigma Research | Swiss Re." 2024. Sigma Research | Swiss Re. April 15, 2024. https://www.swissre.com/institute/research/sigma-research.html.

Shi, Catrin. 2021. "CFC: Real-life Systemic Cyber Events Challenging Model Assumptions | Insurance Insider." Insurance Insider. December 29, 2021. https://www.insuranceinsider.com/article/29eg3lhzopfx8r3rvr2f4/cfc-real-life-systemic-cyber-events-challenging-model-assumptions.

Whittaker, Zack. July 5, 2021. "Kaseya hack floods hundreds of companies with ransomware. Techcrunch. https://techcrunch.com/2021/07/05/kaseya-hack-floodransomware/.

Williams, Chesley. "A Look Back at the 2011 Great East Japan (Tohoku) Earthquake | Moody's RMS." 2021. March 10, 2021. https://www.rms.com/ blog/2021/03/10/a-lookback-at-the-2011-great-east-japan-tohoku-earthquake.

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