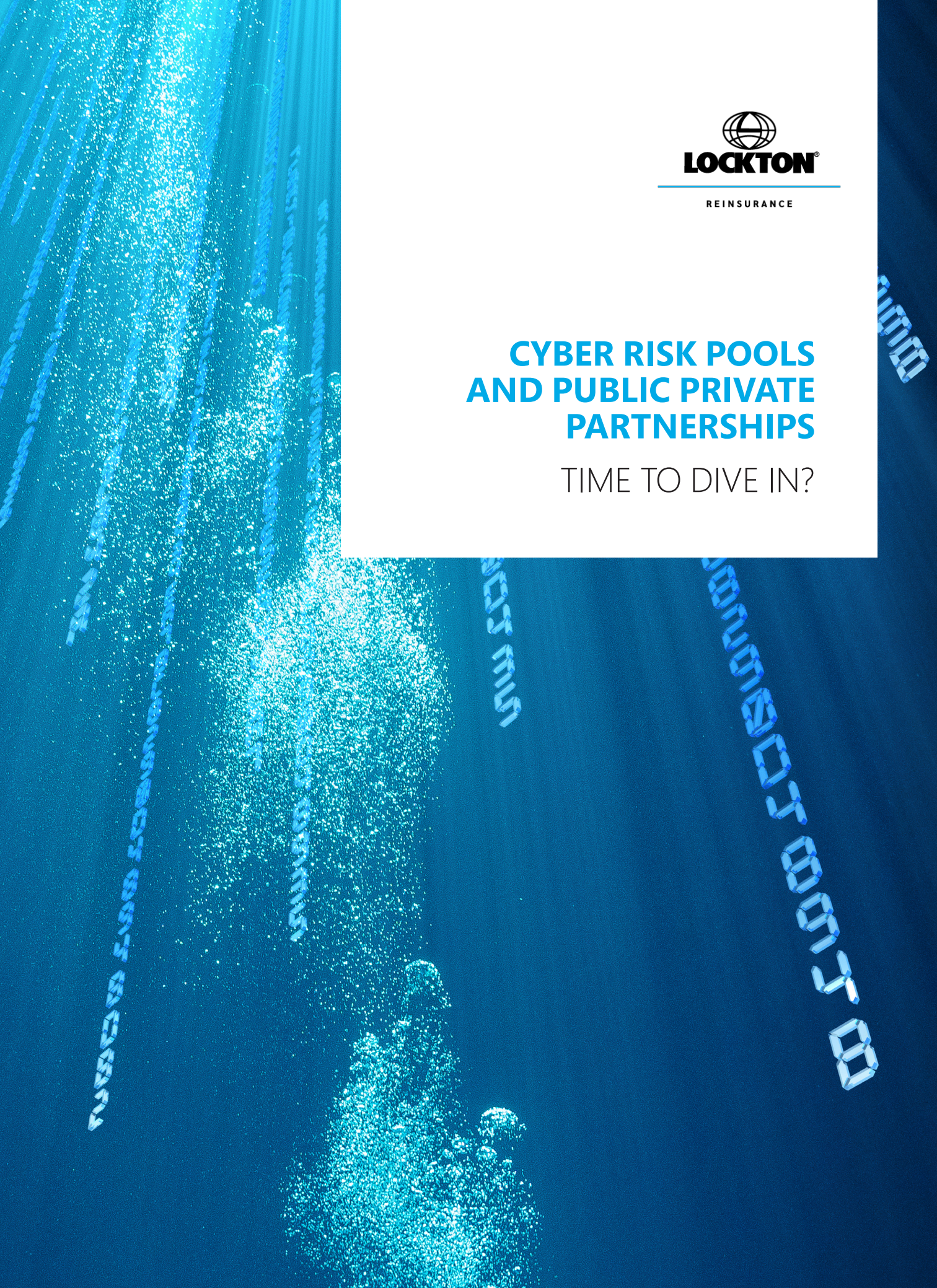


LOCKTON®

REINSURANCE

CYBER RISK POOLS AND PUBLIC PRIVATE PARTNERSHIPS

TIME TO DIVE IN?

- Exposure
- **Peril**
- **Risk Transfer**
- Placement

About Lockton Re

Lockton Re, the global reinsurance business of Lockton Companies, helps businesses understand, mitigate, and capitalise on risk. With over 400 colleagues in 19 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'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. 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.

Executive Summary

In our hyper-connected world, almost every aspect of modern economies is inextricably dependent on technology. The growing wave of artificial intelligence only further increases the potential for cyber-attacks. As a result of this reliance, if a system becomes unavailable, cloud networks compromised, or electronic communications are impaired, there could be massive implications for the financial health of societies.

There have been numerous examples of specific critical sectors of society being impacted by cyber incidents, such as healthcare, transportation, and financial services. There are well documented[1] reports of the extent of these occurrences, with over 420 million attacks impacting over 160 countries during 2023. To date, thankfully such events have been relatively limited in their impact.

An open question remains that if a very unlikely, but potentially very significant cyber event occurs, how should the insurance industry and governments address this challenge? To date, the insurance industry has taken an understandably cautious approach to this issue, using policy exclusions to limit and define the parameters of coverage. The follow up question for the industry is whether this approach is sufficient to remain relevant and address the consequences of a major cyber event.

An open and honest debate is required on the role of governments to support a cyber risk pool to act as a backstop in the face of this peril. We provide an overview of the merits and challenges, and explore what lessons can be learned from precedents and experience in other contexts. It is intended as a sober review of successes and drawbacks in the landscape of public private partnerships (PPP) to support the cyber (re)insurance market and wider society.

The basis and value of a risk pooling mechanism for cyber perils are understood. The next step is to roll up our collective sleeves and continue the hard work of addressing the detail to establish a minimum viable risk pool. Better to start small, and get something up and running which can be refined over time. Understanding the minimum consensus required to create an achievable risk pool is an important principle. Once active, refinement to PPP structures may be needed but having a basis to start with is a lot easier to manage before a cyber catastrophe occurs compared with afterwards.

The paper is organised in the following sections:

- Introduction
- Setting the scene: Precedents and templates
- The Ant and the Grasshopper: Preparation or post-event reaction
- What type of cyber catastrophe would qualify?
- Why support a backstop?
- Evolution and incrementalism: Start small
- Legitimate concerns
- Conclusion

[1] https://www.knowbe4.com/hubfs/Global-Infrastructure-Report-2024_EN_US.pdf

Introduction: Government as insurer of last resort

Volcanos, hurricanes, floods, pandemics, credit shocks, wars and terrorist attacks - catastrophic shock events take many different forms, with dramatic societal and financial implications. Since the industrial revolution, governments have played an undeniably important role in helping society get back on its feet after such events.

Modern governments take on the role of being insurer of last resort in a variety of domains, whether by choice or by default. This is particularly evident where the scale of loss is beyond the scope of a private insurance market, there is underinsurance in society, or the impact would create undue hardship on a segment of the population.

The challenge we currently face relating to systemic cyber risks is that the pace of change has outstripped the mechanisms to manage and mitigate these exposures to society. The limited scope of the private insurance market contributes to the reality of governments acting as de facto insurers of first resort for the most extreme systemic cyber risks, potentially prompting a weakening of economic resilience.

The debate about the role of government in private markets (especially financial markets) has been rumbling on for centuries. Instinctive reactions based on political philosophies, and often visceral, oversimplified arguments rage on both sides. On one side, governments are seen as bureaucratic meddlers, intervening in private markets where they should not. On the other hand, governments with vast resources provide crucial support to areas where financial returns are not prioritised and mitigate market failure. Given the complexity and scale of modern economies, governments play a vital role in providing guarantees to enable risks to be addressed which are deemed beyond the ability or willingness of a market to assume.

The purpose of this paper is not to rehash the broader debate about the role of government, but to shine a light on the opportunities and limitations of a PPP in the cyber insurance market in its current guise. The aim is to explore how to manage the potential impact of catastrophic cyber events and consider a range of interventions. We examine the current state of engagement in PPP and explore the concepts and ideas which have been raised to date.

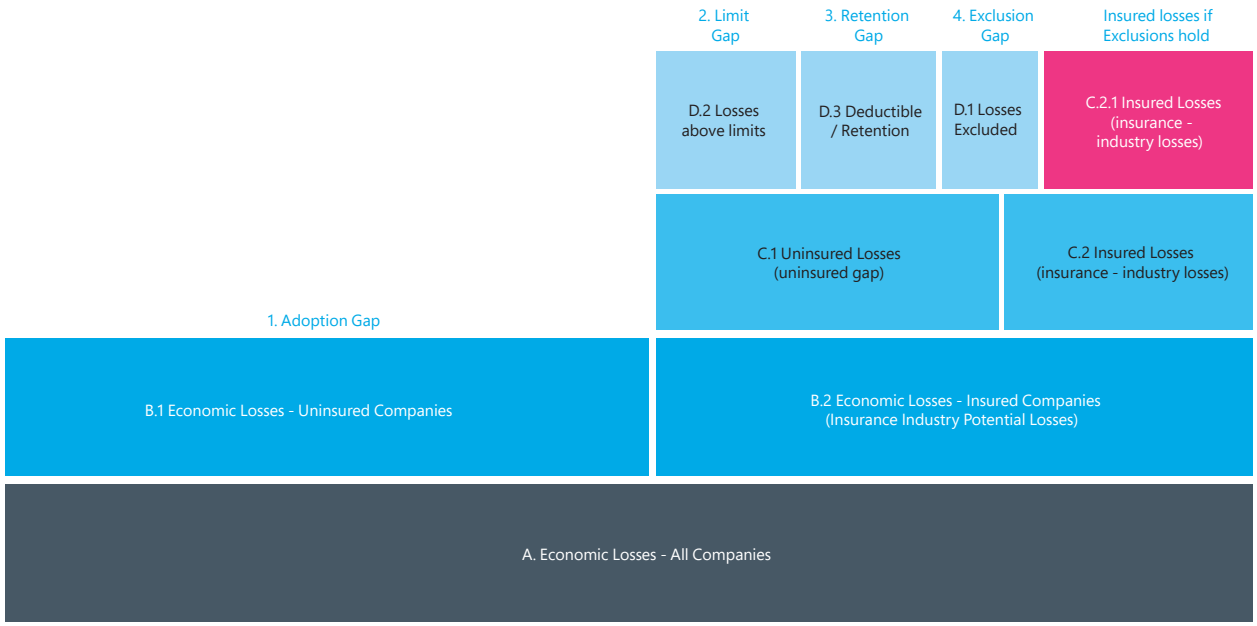
In the context of cyber insurance, a catastrophe is conceivable in the coming years which could far exceed the currently estimated $15 billion premium market. We know that the critical foundational infrastructure of societies such as power, water and health rely on digital connectivity. What if these become threatened? The nature of extremely rare, high-severity events makes these hard to imagine. It is a failure of forethought and imagination not to consider how these events could manifest and what preparations should occur.

Currently, almost all affirmative cyber insurance policies exclude critical infrastructure due to understandable caution by the industry about the extent and ability to manage these losses. Similarly, acts of war conducted by cyber-attack are also excluded (the details of the debate around this topic are out of specific scope of this paper). In this way, the government is in the position of acting as fallback support in the event of a major event or act of war.

The benefit of active engagement in the subject is that potential interventions can be discussed in a clearer and more objective manner that avoids the inevitable skewed perspective in the aftermath of a major event. A reflective view of the topic benefits all involved, and a long-term focus enables priorities to be established. An achievable goal is to set the framework for a risk pool, which can be refined and built upon with governments to enable its enactment.

A solution to address areas of cyber risk not currently insured, such as war and critical infrastructure, is an ambitious though realistic objective. Figure 1 provides an outline of how exposures are currently addressed, illustrating the limited scope of the private market today.

Figure 1: Current state framework of how economic losses are treated (credit: CyberCube)



Setting the scene:
Precedents and templates

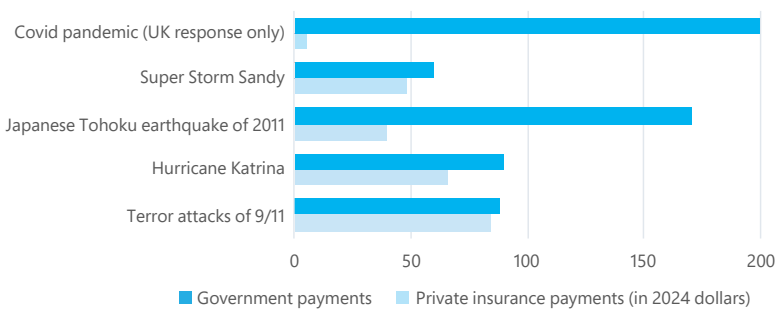
There are numerous examples where governments have stepped in to support communities in times of extreme need, and in many cases have contributed more to the financial recovery following a shock event than the private insurance market. This is particularly evident where insurance purchasing may be limited or coverage restricted.

In almost all instances, pooled funding arrangements between government and industry have developed in the aftermath of a catastrophe. Government working in tandem with the insurance industry has played a critical role in building increased resilience in the face of extreme but rare events. Figure 2 shows some example catastrophe events, and the relative contribution of government compared with private insurance recoveries.

There are several operational, successful PPP schemes upon which lessons can be drawn. They are typically developed in the shadow of a major disaster which has prompted rapid intervention. It does not have to be this way. Planning and consideration allows for carefully thought through schemes which address the key issues, as well as minimise the unintended consequences.

There are essentially two main types of PPP. Firstly, risk distribution (such as Flood Re) enables the sharing of unacceptable risks across a broad pool of financing. This approach enables the mitigation of market failures, for example where insurers choose not to offer coverage due to the loss experience. A second type of PPP explicitly ringfences risk and removes it from the private market. Schemes such as Pool Re enable the most severe losses from physical terrorism to be protected by a separate balance sheet, backed by the UK government.

Figure 2: Lockton Re table comparing private insurance and government financial response to selected twenty first century disasters. Note these estimates do not include indirect losses or lower than expected economic activity.



Flood Re

Flood Re was set up in 2016 in response to the disproportionate and growing impact of flood risk within the UK. Prior to Flood Re, only 9% of homes[2] which had experienced a previous flood were able to obtain an insurance quote from two or more insurers. The coverage provided by Flood Re allows more insurers to offer flood insurance which, in turn, provides more choice for consumers. It is a specific time-bound market intervention and due to expire in 2039. Flood Re was set up by Act of Parliament with the time limitation operating as a catalyst to support the market through a transition as resilience is improved and avoid the market failures which leave individual consumers unable to obtain insurance.

Every home insurer in the UK contributes a levy towards the operation of the scheme, which provides working capital to run the scheme. This raises approximately £135m per year.[3] In addition, there is a fixed premium for each individual flood risk covered in a homeowner policy and included under the scheme. This is based on Council Tax valuation bandings, rather than actual flood risk potential, allowing more affordable premiums for consumers. Valid flood claims from UK home insurers are reinsured and insurers are subsequently reimbursed for losses.

[2] https://www.floodre.co.uk/one-year-flood-re-succeeds-bringing-choice-flood-affected-communities/

[3] https://www.floodre.co.uk/wp-content/uploads/Flood-Re-Annual-Report-2023.pdf

These claims are also subject to an excess of £250 per policy. Currently over 350,000 homes benefit from the Flood Re risk sharing pool, approximately 2% of the UK market. Only homes built prior to 2009 are supported by Flood Re, so as not to incentivise home building in new flood prone areas.[4]

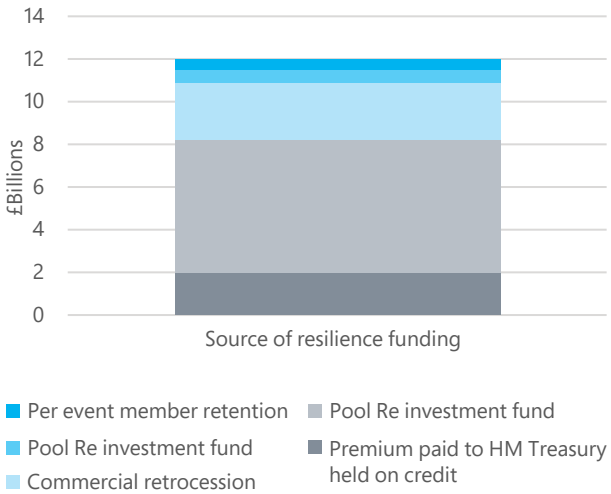
The Flood Re model has been effective, increasing the flexibility of market participants whilst allowing time for flood-prone areas to improve protections ahead of the 2039 exit. It operates as a joint not-for-profit initiative between the government and industry. Benefits of the scheme include material improvements in the availability of flood insurance for consumers, as well as a focused effort to enhance flood defences.

Pool Re

In the early 1990s, a series of terrorist attacks impacted central London, in particular affecting commercial property in the financial district. Property insurance at the time did not contemplate cover for terror risks separately, and cover was automatic as part of an all-risks policy. Insurers were unprepared, and terrorism perils were simply not underwritten. In response, a government backed voluntary reinsurance pool was established to reinsure the terrorism exposure for property risks. In turn, the UK Treasury (HMT) backed the contingent liabilities of Pool Re and committed to cover any losses beyond the funds of Pool Re, by loaning the funds to Pool Re to provide confidence to the industry.

In return for this backstop, HMT receives a portion of premiums. Since 2015, Pool Re has contributed over £2 billion to the treasury, and has never made a call on the guarantee since inception of the scheme. Since the founding of Pool Re, the scheme has built up an investment fund of over £7 billion. Pool Re purchases commercial retrocession, there is a per event member retention, and premium paid to HMT is held in credit, all of which creates a substantial financial buffer, making the potential of a claim on government funds extremely remote. As illustrated in figure 3, the aggregate funds before government involvement of approximately £12 billion represents an estimated modelled return period of 1:1,500.

Figure 3: Pool Re funding and reserves[5]



One of the long-term goals is to expand and integrate the terror cover available to small and medium sized companies, which currently only have 4% of this group purchasing specific terror cover. By providing unique capacity to low frequency events, it improves the solvency position of the market because, without Pool Re, individual insurers would be required to hold additional capital to meet solvency requirements.

Pool Re has built up strong experience and expertise in addressing this risk and is able to offer risk management support to its members, further reducing the risk burden on the government, and improving societal resilience. Pool Re is also able to use a portion of the funds to invest in resilience programs, in conjunction with the government and police, to minimise and mitigate the impacts of terror attacks.

Australian Reinsurance Pool Corporation

The Australian Reinsurance Pool Corporation (ARPC) was set up following the Terrorism Insurance Act of 2003, and is a public financial corporation to run reinsurance for specific extreme perils on a not-for-profit basis. The program allows domestic insurers to elect to purchase reinsurance for eligible risks through ARPC at competitive rates, with the additional benefit of a $10 billion government backed guarantee, beyond the significant buildup of funds in the Pool.

[4] How Flood Re Works, (Website) https://www.floodre.co.uk/how-flood-re-works/

[5] PoolRe-Annual-Report-2023-2024-.pdf

In the event of a "declared terrorist incident", terror exclusions in standard policies are overruled to afford coverage for those participating in the scheme.

In 2022 this was expanded to include cyclone related flood damage. The expansion to incorporate coverage for cyclones was compulsory for domestic insurers, with large insurers required to join prior to the end of 2023, and small insurers prior to the end of 2024. Once the Australian Bureau of Meteorology declares a cyclone has occurred, related claims are covered for the cyclone's duration and 48 hours afterwards.

Built into the scheme is a periodic review of the merits of the program (currently every 3 years). The most recent report in 2021 [6], reaffirmed the value of the ARPC to mitigate potential market failure, due to the insufficient availability of terrorism insurance at reasonable rates. Interestingly, physical damage arising out of cyber terrorism was considered for inclusion in the pool and at the time of the review was recommended not to include it. The main reasons cited for continuing to exclude cyber-physical coverage were:

- cyber physical risk cover could further reduce the appetite of those providing retrocession for the ARPC.
- The cyber insurance market is still rapidly evolving in Australia, and insurers do not currently provide physical damage cover. If the ARPC offered this, it would increase expectations that Australian insurers would offer "all-risks" cover and make it hard to compete with the government backed program.

The ARPC has effectively helped support and maintain the stability of the terror insurance market. By adding cyclone and flood cover, it brings together a mutuality for perils which are low frequency, potentially high severity and hard to model. Resilience is improved through mitigating the worst impacts of a major event.

Terrorism Risk Insurance Program (TRIP)

The unprecedented terror attacks of 9/11 changed the course of history, as well as the insurance industry. In the wake of massive terrorism losses, which were not contemplated on the scale suffered, a government backed program was set up. Political will supported the Act of Congress in 2002 to create the Program. It has been reauthorized since, with various updates and amendments to adapt to the changing requirements of the program. This includes:

- Nine data calls relating the volumes of premium in different industry sectors
- Updates to modelling tools and evaluation of the impact of certified of terrorism
- Changes to the coinsurance, insurer deductibles and overall structures.

TRIP has enabled wider availability of terror insurance and restored market confidence following the major disruptions to the market in the wake of 9/11. The principle of sharing significant ongoing financial risks has endured and enabled the US government and the private insurance market to provide support for complex, hard-to-quantify risks with an uncertain tail exposure.

[6] https://treasury.gov.au/sites/default/files/2021-12/p2021-230249-review-final-report.pdf

The Ant and the Grasshopper: Preparation or post-event reaction

The famous Aesop fable represented in figure 4 tells the story of the grasshopper who plays music all summer, while the ants are busy working hard gathering food for winter. When the grasshopper begs for food and shelter, it is refused by the ant. The benefits of preparation and planning in the context of foreseeable, if unlikely, events have a compounding positive ripple effect across the insurance industry and society broadly. Getting ahead of a potential catastrophic event, which ultimately lies at the feet of government, where not covered by private insurance markets, is prudent.

An example of assessment of contingent liabilities is a 2020 HMT report[8] which reviewed how these are treated and outlined proposals for improvement of the management of these risks.

There are four key objectives outlined in the report:

1. improve the expertise in the government to quantify and price risk
2. improve compensation for risk taken on by the taxpayer
3. establish the right incentives to reduce both the probability of risk materialising and the cost when it does
4. clarify risk ownership to provide more certainty on how losses will be shared between the Exchequer, departments and the private sector

This provides a good foundation for consideration of contingent liabilities that exist across different sectors. There are valuable themes and lessons to be drawn from the various types of shared risk pooling efforts and collaboration between governments and private (re)insurance markets.

- Schemes have been developed for rare, uncertain, low frequency perils which have the potential to manifest in significant economic and societal impact
- If the event(s) were to occur, in addition to the financial impact, there could be implications for the confidence of the insurance market
- There are limited historical events to build experience-based models for insurance risk assessment
- Maintaining adequate capital for these types of events is expensive, and insurance coverage would be more limited and less available without these pools
- Once established, risk pools encourage improved financial and societal resilience

In the last two decades alone, western economies have seen major financial shocks arising from the global financial crisis, the Covid-19 pandemic and the energy security crisis following the invasion of Ukraine. The required fiscal intervention by governments has

Figure 4: The Ant and the Grasshopper [7]

created long term structural challenges for economies, inflationary pressure and limited the scope of government ambitions. The insurance industry has the opportunity to play an important role to lead the conversation in resilience and preparedness.

Since the nascent years of the cyber insurance market, the concept of a government backstop has been an ongoing topic of interest.

In November 2012, when estimated global cyber insurance premium was less than $1 billion, the US department of Homeland Security published a paper[9] called the Cybersecurity Insurance Workshop Readout Report, which referred to the merits of a government role in supporting cyber related events that are outside the risk appetite of the insurance industry.

[7] By Charles H. Bennett 1857 - https://en.wikipedia.org/wiki/The_Ant_and_the_Grasshopper

[8] https://assets.publishing.service.gov.uk/media/5e67c54e86650c727b2f46d6/06022020_Government_as_Insurer_of_Last_Resort_report__Final_clean_.pdf

[9] https://www.cisa.gov/sites/default/files/publications/November%25202012%2520Cybersecurity%2520Insurance%2520Workshop.pdf

Since then, both the breadth and scale of technology interconnectivity, as well as the associated cyber insurance market have grown dramatically. Coverage has expanded in a competitive and open market environment. There have been numerous 'near miss' events which acted as catalysts for governments to consider the likelihood and severity of potential catastrophic events more closely – including the scale at which government support would be needed. Even the most conservative estimates[10] suggest that the market will be capital constrained in the next few years, without significant additional capital from a range of sources. Because of ongoing digitisation, the expectation is that cyber risk will become a major exposure for society in the next few years, so capital required will outstrip current levels, unless new entrants continue to support the market.

Rebecca Bole, head of strategic partnerships at CyberCube has been exploring the future role of capital for the growth of the market. She states: "Cyber insurance is projected to grow rapidly over the next decade, becoming a peak peril. Collaboration between government and the insurance industry in preventing, mitigating, and responding to catastrophic cyber risk is the only way societies can remain resilient."

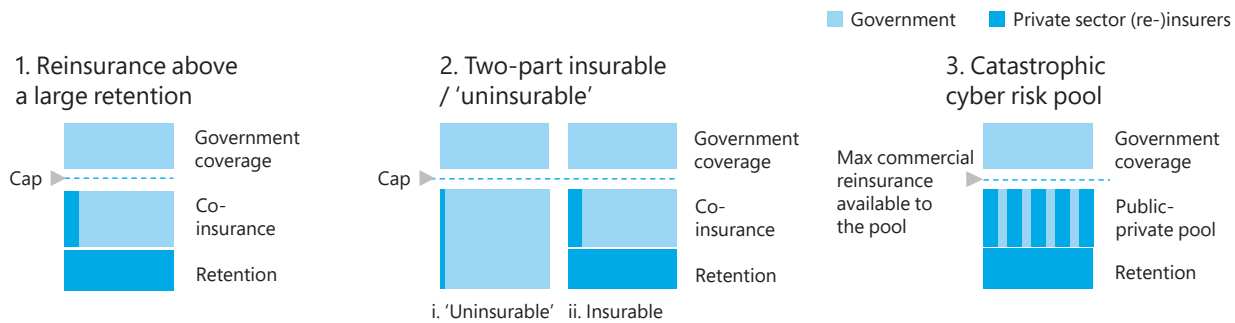
In recent years, discussions between the insurance industry and government have increased, particularly in the US and the UK. In the US, discussions have involved the Federal Insurance Office, part of the US Treasury, whilst in the UK, Pool Re, the successful terror reinsurance pool backed by HMT, has contributed to industry thinking by sharing proposals for a PPP to address systemic cyber risk with industry participants.

Josephine Wolff, Associate Professor of Cybersecurity Policy at Tufts University suggests: "There's a general expectation that in the event of a catastrophic cyber-attack, the government would probably help pay for the resulting damage and recovery. But we don't have a clear understanding of what the government would consider a catastrophic cyber-attack or what form that help would take."

There is an emerging consensus of what the challenge to be addressed is, and the need for partnership between industry and government. Understandably, major questions exist about the nature and mechanics of how it may operate. Given the limited adoption of cyber insurance by small and medium sized businesses, encouragement by government to increase adoption will build resilience. Topics of legitimate debate include how it would be funded, its structure, what threshold would trigger coverage, what requirements are needed of insurers to participate, and how the coverage would operate.

Given the pace of change in the cyber insurance market, any scheme needs to enable and encourage continued innovation and evolution of the market. Any structure which stifles the market or mandates an approach will not be successful. Another key issue in the design of any government-backed national pool is how to impose geographic boundaries around a peril that does not respect them.

Figure 5 : Potential structures setting out options for a cyber risk pool (credit: CyberCube).



[10] https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/about-cyber-insurance-market.html

Figure 5 on page 10 shows example structures and different ways to address the interaction between sources of private and public capital. The first approach suggests a distinct line between where the private market ends, and government protection begins. One challenge with this approach is that it may create distortions for the private market as government protection may skew incentives for private catastrophe cover. The second approach draws a distinction between "uninsurable" events (such as cyber war) which are currently outside the scope of the private market, so would be addressed by government cover, and other exposures covered by the market. This may have unintended consequences that private market coverage becomes narrower in the context of a parallel government cover. One objective of any PPP should be that it encourages broader and deeper participation in the private market rather than less support. The third suggested structure involves a PPP which creates a financial buffer for the private market, and a government guarantee (rather than affirmative coverage) to support this. Currently this third approach has the most support behind it and the highest chance of coming to fruition.

What kind of cyber catastrophe would qualify?

The types of event, which could be serious enough to require a cyber backstop are extremely rare. These tail risks include examples below:

- Cascading cloud outage caused by a malicious actor, most likely affiliated with a nation-state
- A self-replicating malware, which spreads rapidly such as via supply chain software, impacting a widely used operating system
- An attack on a critical national infrastructure, such as electricity power supply, or key technology which supports major elements of the economy

The concept of a backstop would require several elements to operate:

- **Geographic boundaries:** There would need to be a clear understanding of how a geographic demarcation would operate. Notwithstanding international company trade, at least initially the simplest alignment currently is along national boundaries, so that the backstop would support companies registered and operating within a particular jurisdiction
- **Trigger:** Rather than navigating the complex and challenging issue of attribution of a cyber-attack, some such as Pool Re, have proposed a parametric trigger based on the impact of the event(s)
- **Financial threshold:** There would need to be a significant aggregate financial impact to act as a threshold for the backstop, and an independent agency to calculate the financial impact
- **Rules for participating:** (Re)insurers which participate would need to agree to a set of criteria regarding ways to continue improving cyber resilience. Examples include:
  - Minimum underwriting standards on a proportional basis to improve risk measures
  - Minimum two way data sharing to improve insurance industry insights
  - Clarity of roles and responsibilities between government, independent risk pool and insurance industry

Why support a backstop?

The concept of a backstop has multiple potential benefits. At its most foundational, a backstop would provide valuable confidence in the market, and encourage broader participation in the (re)insurance market. This ultimately could increase competition to the benefit of buyers, as well as reduce relative pricing as additional entrants join the cyber market. Another benefit is that participation in any backstop would enable improved alignment of what constitutes cyber security best practice, with minimum standards part of the equation to encourage good cyber hygiene.

A cyber risk pool should facilitate the market's expansion, with a corresponding dynamic financial attachment threshold, which increases with market growth. (Re)insurers can influence the critical aspects of technology, processes and protocols which are correlated with lower risk and more resilient outcomes. In turn, coverage can expand over time to address a wider set of perils, and increase capital deployment. Josephine Wolff comments: "Setting up a government response to catastrophic cyber risk in advance would allow the government to impose certain requirements or security standards for participants, raising the bar for cybersecurity across industry, and reducing the risk of a major incident. Something that simply won't be possible to do in the same way if such a program is worked out after a catastrophic event has already occurred."

Over time, a backstop has the potential to become a material asset for those supporting it, including governments. The example of Pool Re in the UK illustrates this; it has amassed a fund of over £7 billion, in addition to the various buffer layers of protection. These pooling arrangements can provide a regular annual income to governments in the form of investment returns, dividends, and premium contributions. In this way, the government balance sheet is effectively used to achieve an important goal for the insurance industry while also providing income for the risk that is assumed. The reality is that governments have an implicit default responsibility in the event of a major cyber catastrophe, so a pooling arrangement allows governments to monetise this exposure, whilst simultaneously creating additional layer(s) of protection from payouts.

As part of a wider value proposition, a backstop structure could be used as a source of effective education and cyber resilience building. Pools such as Flood Re provide support to local communities and insurance brokers with resources about flood protections and resilience. In the same vein, a cyber risk pool could lead the way in better understanding both the building blocks of cyber security, and the potential impact of high severity cyber catastrophes.

Evolution and incrementalism: Start small

To have a meaningful conversation with government, even just to explore options available, building insurance industry consensus will be important. The basis for developing anything which has the potential to involve taxpayer funds, however remote the likelihood, can be emotive and challenging. An event big enough to impact a backstop is extremely unlikely and building support for this type of structure requires a recognition of the art of the possible, and a level of pragmatism.

An understanding of the various trade-offs and the external factors which influence the ability to get the idea off the ground is needed. In utilitarian terms, one approach is to focus on the broadest pool of companies which would benefit from a cyber risk pool and prioritise small and medium businesses. These companies are less likely to have robust cyber security procedures in place, and may be more prone to the impacts of an extreme cyber event. In this framing, the companies impacted could receive some protection via participating insurers, without a detailed assessment of specific individual claims.

An alternative approach is to base any backstop on the key perils it addresses. "Critical technology infrastructure", such as cloud providers, major internet backbone cables, mobile communications and similar, both private and state owned, constitute key components of a functioning economy. A backstop could cover certain impacts on these services as the trigger for support, in addition to a financial threshold. This would mean that these core infrastructure assets would benefit from government backed protection so that insured companies relying on them, irrespective of size, would benefit from cover. Part of the estimation in establishing a risk pool is that broader cover with fewer exclusions could be offered.

Mark Camillo, CEO of CyberAcuView states: "There are potential shared benefits between the insurance industry, policyholders and governments with a program that could address some of the gaps in coverage today, particularly as it relates to critical infrastructure, in addition to the expansion of the existing market with a government backstop for extreme events."

As recognition of the growing importance of data centres, in September 2024 the UK government formally designated them as part of critical national infrastructure[11]. This means they now enjoy the same status as energy and water companies, as well as emergency services. The Technology Secretary Peter Kyle MP said[12]: "Bringing data centres into the Critical National Infrastructure regime will allow better coordination and cooperation with the government against cyber criminals and unexpected events."

This action acknowledges the existing implicit responsibility which the government already has for these services, fundamental to our society.

Any cyber backstop scheme which has a compulsory element to it, will inevitably be more challenging to approve and set up, as well as include a higher cost to establish. For this reason, there is a better probability of success if any scheme initially focuses on a voluntary approach to the backstop.

[11] https://www.gov.uk/government/news/data-centres-to-be-given-massive-boost-and-protections-from-cyber-criminals-and-it-blackouts
[12] ibid

Legitimate concerns

There are legitimate concerns which have been expressed about the principle of a backstop, as well as the many complexities and practicalities of enacting one.

One fundamental criticism whether the premise for the need of a cyber backstop is correct. The discussion around a backstop assumes that a cyber event could occur which is outside the appetite of the insurance market, or larger than the private insurance market can cover. If this is not the case, it could be deemed unnecessary. Given that a cyber catastrophe warranting a backstop has not yet occurred, this is an issue which will continue to create challenges for policy makers. However, the fear alone of a cyber catastrophe is enough to create hesitation among capital providers and could become an inhibitor to growth.

The process of planning and preparedness can improve the ability of the private market to respond, as well as the resilience of those affected. Josephine Wolff states: "Given the wide range of different forms that cyber intrusions and attacks can take, there's an advantage to laying out ahead of time what types of incidents the government anticipates providing support for so that insurers and their policyholders are not left wondering and so that those decisions aren't being made in haste, in the immediate aftermath of a major crisis."

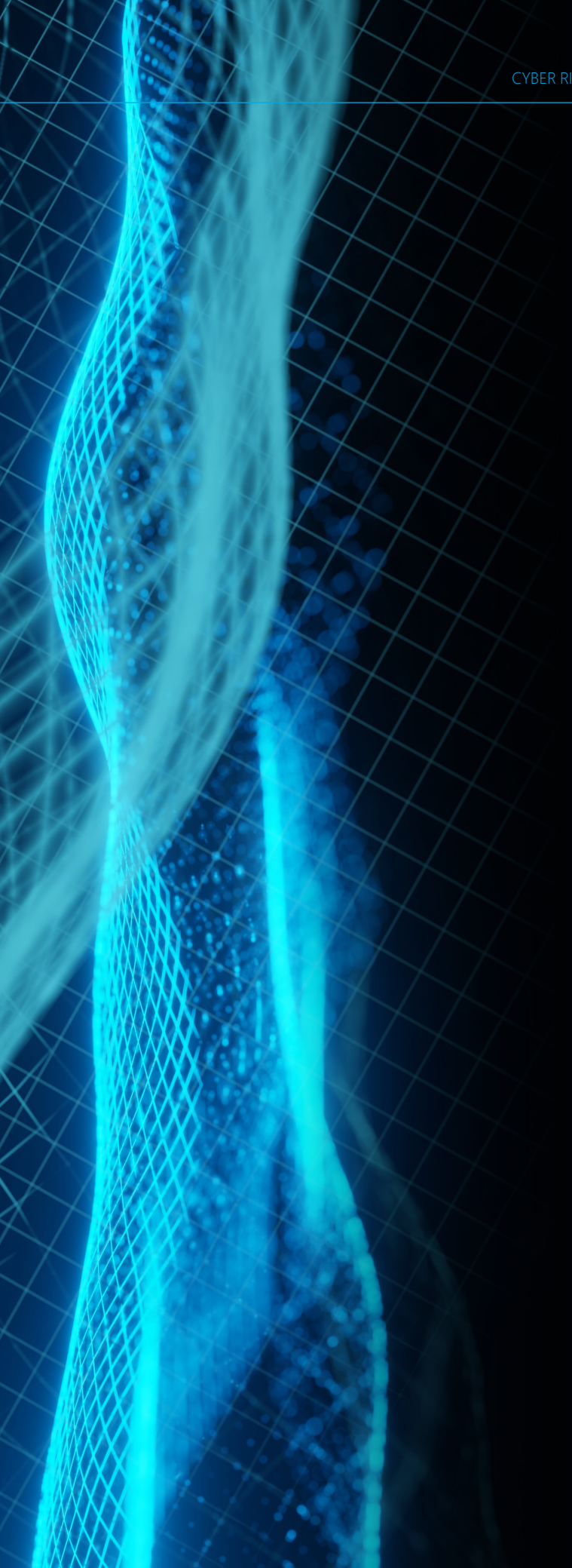
A second specific area of concern is that inconsistency in coverage caused by those who join the backstop and those who do not, could lead to uneven loss impact in the event of a cyber catastrophe. This can be alleviated with a common approach to minimum standards and creating the appropriate incentives for the industry to participate in a voluntary program, which can be adopted over time, and so avoid creating undue market distortion. These standards could build upon successful public education programs such as the Cyber Essentials[13] in the UK and other international risk-based standards such as the NIST Cybersecurity framework[14].

A third issue which has been debated is the threshold at which a cyber event is truly systemic and should trigger a backstop. One organisation which is helping to address this is the Cyber Monitoring Centre[15] (CMC). The goal of the CMC is to provide an independent and objective categorisation of cyber catastrophes on a scale of one to five, based on how widespread they are and their economic impact. This can be used by the (re)insurance industry to tailor coverages for extreme events. The clarity brought by a rating scale for cyber events could attract more private capital to the market, and governments need only be there for events which are truly too big for the private market to handle.

Experts suggest that the CMC could easily extend and adapt its categorisation scale to align with the agreed thresholds for any government backstop. The organisation is in its early stages of evolution, and currently has a UK geographic boundary, though there are steps to potentially expand this into other territories such as the USA where cyber insurance is more widely adopted. The CMC can act as a mechanism not only for (re)insurers in tailoring cover for catastrophic events but also for government backed pools in triggering them. If there is uniformity in classification system, back-to-back risk transfer solution can emerge, ensuring organisations don't face a protection gap when it comes to systemic cyber risk.

Finally, given the rapid speed of the cyber market evolution, some argue that the basis of what should be covered in any backstop is not yet settled. As technology will continue to transform society, this will be a perpetual issue. As a result, this is not a sufficient reason to postpone addressing the issue. Indeed, it can be argued that this challenge will become harder to address over time as the market becomes larger and more established so better to tackle this head-on when the market has less scale.

[13] https://www.ncsc.gov.uk/cyberessentials/overview
[14] https://www.nist.gov/cyberframework
[15] www.cybermonitoringcentre.com



Conclusion

The merits of a cyber risk pool are clear: its time has come. While the concept of a backstop is contentious in some quarters, and execution of the details complex, the merits of working through the thorny challenges from idea to fulfilment make it worthwhile. There are many staging posts along the journey to achieving a sustainable objective but, given the increasingly challenging cyber risk threat landscape, the benefits of planning ahead are substantial.

The experience of Covid-19 alone illustrates the inefficiencies, unintended consequences and at times wasteful impact of government fiscal support following an event, when used as a blunt instrument without appropriate forethought. Other PPP initiatives showcase the advantages and stability to specific insurance markets.

A risk pool allows orderly engagement with the process, rather than a chaotic and urgent response after a catastrophe. With the potential for massive, though unlikely, events increasing due to the critical reliance on technology, a backstop provides part of an effective partnership between the private cyber (re)insurance market, and respective key governmental bodies. A government-backed cyber risk pool arrangement in isolation is not a panacea. However, in conjunction with other measures including ongoing improvements to security standards, it can form a major support in building societal resilience and closing the cyber protection gap.

Authors and Contacts

AUTHORS

London

Oliver Brew ACII
Cyber Practice Leader, International

+44 (0)7384 248 268
oliver.brew@lockton.com

New York

Brian Lewis
Cyber Practice Leader, North America

+1 646 279-1940
brian.lewis@lockton.com

CONTACTS

London

Matthew Silley FIA
Senior Broker

+44 (0)7391 387 699
matthew.silley@lockton.com

Annie Terry ACII
Broker

+44 (0)7446 892844
annie.terry@lockton.com

Jemima Hopper ACII
Broker

+44 (0)7855901856
jemima.hopper@lockton.com

New York

Mark Braithwaite
Co-Leader – North America Casualty & Financial Lines

+1 646 901 9241
mbraithwaite@lockton.com

Emily Apostolides
Co-Leader – North America Casualty & Financial Lines

+1 347 534 8850
eapostolides@lockton.com

Andrew Bilello
Senior Broker

+1 516 269 0974
abilello@lockton.com

Pat Sweeney
Broker

+1 646 628 3088
psweeney@lockton.com

MEDIA CONTACTS

Isabella Gaster
Lockton Re Global Head of Marketing

+44 (0)7795 400981
isabella.gaster@lockton.com

Elizabeth Miller Kroh
Lockton Re Head of Marketing,
North America

+1 (445) 248 2228
elizabeth.kroh@lockton.com

ACKNOWLEDGEMENTS

This paper would not be possible without the review, contributions and suggestions from several people around the cyber insurance industry. Some prefer to remain anonymous, and we acknowledge their input and perspective. Others who have provided feedback and advice are:

Josephine Wolff
Associate Professor of Cybersecurity Policy at Tufts University

Rebecca Bole
Head of Strategic Engagement, CyberCube

James Burns
Head of Cyber Strategy, CFC

Mark Camillo
CEO at CyberAcuView

Will Mayes
Managing Director at QualRisk

Sources

1. KnowBe4. (2024). Cyber Attacks on Infrastructure.The New Geopolitical Weapon. https://www.knowbe4.com/hubfs/Global-Infrastructure-Report-2024_EN_US.pdf

2. Cox, E. (2017, April 4). One Year on: Flood Re succeeds in bringing more choice for flood affected communities - Flood Re. Flood Re. https://www.floodre.co.uk/one-year-flood-re-succeeds-bringing-choice-flood-affected-communities/

3. Flood Re Limited, Hoban, M., Bord, A., Eden, J., Green, S., Logue, S., Sharp, J., Stedman, S., Thomas, P., & Boughton, H. (2023b). Annual report and financial statements. In Annual Report and Financial Statements [Report]. https://www.floodre.co.uk/wp-content/uploads/Flood-Re-Annual-Report-2023.pdf

4. How Flood Re works - Flood Re. (2024, October 2). Flood Re. https://www.floodre.co.uk/how-flood-re-works/

5. Pool Reinsurance Company Limited. (2024). Annual Report 2023–2024. https://assets.poolre.co.uk/sitefiles/2024/08/PoolRe-Annual-Report-2023-2024-.pdf

6. Commonwealth of Australia, & Sukkar, M. (2021). Terrorism Insurance Act Review. https://treasury.gov.au/sites/default/files/2021-12/p2021-230249-review-final-report.pdf

7. Wikimedia Commons (2024). The Ant and the Grasshopper by Charles H. Bennett (1857). https://commons.wikimedia.org/w/index.php?curid=14706290

8. Crown copyright. (2024). Government as Insurer of Last Resort: Managing Contingent Liabilities in the Public Sector (2020). https://assets.publishing.service.gov.uk/media/5e67c54e86650c727b2f46d6/06022020_Government_as_Insurer_of_Last_Resort_report__Final_clean_.pdf

9. U.S. Department of Homeland Security & National Protection and Programs Directorate. (2012b). Cybersecurity Insurance Workshop: Defining Challenges to Today's Cybersecurity Insurance Market. https://www.cisa.gov/sites/default/files/publications/

10. Swiss Re. (2024). Cyber Insurance Market Report 2024. https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/about-cyber-insurance-market.html

11. Department for Science, Innovation and Technology. (11.09.2024). Data centres to be given massive boost and protections from cyber criminals and IT blackouts. https://www.gov.uk/government/news/data-centres-to-be-given-massive-boost-and-protections-from-cyber-criminals-and-it-blackouts

12. ibid

13. National Cyber Security Centre. (2024). Cyber Essentials. https://www.ncsc.gov.uk/cyberessentials/overview

14. NIST. (2024). Cybersecurity Framework January 2024. https://www.nist.gov/cyberframework

15. CMC. (2024.) Cyber Monitoring Centre. https://www.cybermonitoringcentre.com/

www.locktonre.com

261 Fifth Avenue, New York • NY 10016

The St. Botolph Building, 138 Houndsditch • London EC3A 7AG

#0558_02.25