Insurance Council of Australia

6 August 2021

The Treasury
Langton Crescent
Parkes ACT 2600

By email: FSD.TIAreview@treasury.gov.au

Dear Premier

SUBMISSION TO THE REVIEW OF THE TERRORISM INSURANCE SCHEME

Summary

The Insurance Council of Australia (ICA) welcomes this opportunity to provide a submission to the Review of the Terrorism Insurance Scheme (the **Scheme**).

The ICA is the representative body of the general insurance industry in Australia and represents approximately 95 percent of private sector general insurers. A foundational component of the Australian economy, the general insurance industry employs approximately 60,000 people, generates gross written premium of $53.9 billion per annum and on average pays out $166.2 million in claims each working day ($41.5 billion per year). In respect to the terrorism insurance scheme, our members underwrite property risks, business interruption and cyber insurance. We also represent reinsurers in the Australian market.

This submission responds to the questions raised in the Review's terms of reference.

1. ***To what extent, if any, is terrorism cover available in the private market on commercially reasonable terms?***

2. ***If there is insufficient private market capacity for terrorism insurance in Australia, what are the barriers to its provision and is the presence of the ARPC hindering the development of commercial terrorism insurance in Australia?***

The ICA maintains the view that there is an ongoing need for the Scheme to continue offering reinsurance for terrorism cover in respect to commercial property (including contents) and business interruption. Terrorism is considered a largely uninsurable risk due to the inability to predict and therefore price for an event. As a result, determining the amount of capacity required remains challenging. This aligns with the findings of each previous triennial review of the Scheme.

Although global reinsurance capacity to address terrorism risk has grown, access to consolidated capacity in Australia has been enabled solely by the operation of the *Terrorism Insurance Act* 2003 (the Act). The capacity of the Australian Reinsurance Pool Corporation (**ARPC**) to amalgamate risk assessment and provide rating and insurer access to guaranteed reinsurance for the terrorism risk continues to be necessary to deliver commercial terrorism cover. The ARPC now provides reinsurance cover to more than 220 insurer customers, which highlights the success of the Scheme.

Reinsurers have reiterated that the pool managed through the ARPC remains the most efficient way for global reinsurers to manage commercial lines exposure to terrorism in Australia. Through the ARPC, global reinsurers are able to centrally support the Australian market with specific reinsurance/retrocession capacity. Without the capacity of the ARPC to funnel the risks into a central pool, it is unlikely that reinsurance capacity would be made available by reinsurers and the situation would revert back to the 'market failure' position post Sept 2001.

Although it is now possible for insurers to obtain reinsurance for terrorism from the global reinsurance market, the operation of the ARPC centralises this purchase and thus makes it easier to bulk-buy cover. The APRC also provides stability in cost for insurers, which in turn provides stability for policyholders.

3. To what extent, if any, is cover for cyber terrorism resulting in physical property damage available in the private market on commercially reasonable terms?

Physical damage from cyber remains an emerging risk which has the potential to cause significant damage to property and consequential economic harm. Recent notable incidents include:

- Power Grid Sabotage, Ukrainian (2015). Hackers gained access to the power grid and disabled electricity to a significant portion of Ukraine. No direct physical damage, although likely to have resulted in indirect physical damage.
- Unidentified steel mill, Germany (2014). Hackers gained access via a ‘spear fishing’ attack that resulted in a staff member downloading malware. The ability to shut down a blast furnace was disabled which caused significant physical damage.
- Natanz uranium plant, Iran (2010). Malware was installed which targeted Siemens industrial control systems (ICS). This caused centrifuges to spin out of control and break, causing significant damage.
- BTC Pipeline, Turkey (2008). The ICS was hacked and alarms were shut down before super pressurising the pipeline, resulting in an explosion. 30,000 barrels of crude oil were spilled.
- Maroochy Water Services, Australia (2000). The industrial controlled system was hacked to release 264,000 litres of sewage across a number of locations. Perpetrated by a disgruntled employee of the company that supplied the ICS.

Notwithstanding the above examples, physical damage remains a remote, albeit growing risk. Critically, it’s a risk that commonly exists in a gap between traditional commercial insurance products. Typical commercial property insurance exclude loss from cyber or data theft. Conversely, cyber insurance policies commonly exclude physical property damage. It follows that commercial businesses with typical insurance cover may not be covered for property damage resulting from a cyber incident.

In response to emerging coverage gaps, industry typically develops new products to cover the risk. This has begun in respect to physical damage from cyber with a limited number of specific product offerings in certain circumstances. However, there remains a high level of uncertainty in respect to pricing of the risk and exposure is difficult to quantify. Additionally, accidental cover of the risk via ‘silent cyber’ cover is being tightened across the market.

Insurers also report difficulty placing adequate reinsurance due to capacity limitations in the private market. Although this capacity may increase, it is currently inadequate to cover a large scale cyber-attack damaging physical infrastructure.

It follows that the ICA no longer opposes an expansion of the Scheme to include physical damage from cyber and we note some insurers advocate for such an expansion. We also acknowledge the research conducted by APRC in recent years to investigate the risk posed by cyber and how this can be effectively addressed by the Scheme.

4. If there is insufficient private market capacity for cyber terrorism causing physical property damage insurance in Australia:

a. What are the barriers to its provision?

b. How would the presence of the ARPC impact the development of commercial terrorism insurance in Australia?

c. Are there international examples of market or policy responses to cyber terrorism causing physical property that are applicable to the Australian context?

If the Scheme is expanded to include physical damage from cyber, there are several barriers that must first be overcome. In effect, Treasury will need to engage in policy amendment beyond simply voiding terrorism exclusions. The Act would either need to void data exclusions in commercial property policies or void property damage exclusions from cyber insurance policies. This is a significant expansion and careful consideration is required to avoid unintentional outcomes.

Additionally, pricing of the cyber risk component of the Scheme requires further consideration. The current Scheme prices risk based on the postcode of the insured asset. This is appropriate for underwriting conventional terrorism where assets located in the CBD of capital cities have the greatest exposure. In contrast, the cyber risks vary based on the industry of the asset and its reliance on an ICS, not the postcode in which the asset is located. For instance, the greatest risk of direct physical damage from cyber is faced by specific industries such as infrastructure, mining, energy and telecommunications. Often these assets located in lower risk tiers under the current Scheme and therefore attract a lower premium.

Conversely, many other businesses face a very low risk of direct physical damage from cyber as their physical assets do not rely on an ICS (or only to a limited extent). This would include many commercial property assets located in Tier A, which attract the highest premium. For example, an office tower in the Sydney CBD may have only a very limited exposure to a cyber incident causing direct physical damage, compared to an infrastructure asset that is highly dependent on an ICS.

It follows that, if the Scheme were extended to include physical damage from cyber, there is a risk that businesses that attract the highest premium under the current Scheme have low exposure to the risk. Consequently, these policyholders may end up subsidising infrastructure that carries a significantly higher risk but attracts a lower premium.

Difficulty declaring a cyber incident as terrorism

Another issue to consider is how the Scheme would respond to a cyber incident and whether a terrorism declaration is appropriate. For the Scheme to apply, the Minister must be satisfied that a ‘terrorist act’ - in accordance with s.100.1 of the Criminal Code - has occurred. The code defines a terrorist act as an act that:

Insurance Council of Australia

intends to coerce or influence the public or any government by intimidation to advance a political, religious or ideological cause.

In the limited publicised instances of physical damage from a cyber attack, often the identity and motive of the perpetrators remain unknown. In many cases, state-sponsored acts of aggression are suspected - which would likely be excluded in most insurance policies under a 'war exclusion' regardless of a terrorism declaration. In other instances, the incident may have been caused by a disgruntled employee or the result of corporate espionage for the purpose of causing financial harm or benefiting from financial gain, which arguably does not constitute terrorism.

In a practical sense, were the Scheme to expand to include this risk, and an incident were to occur, the Minister may be placed in the position of having to make a binding declaration when the motives of the perpetrator remain unknown. This potentially risks expanding the definition of terrorism.

Potential betterment opportunities in restoring physical property

Although beyond the scope of this review, if the Scheme is expanded to include physical damage from cyber, ARPC should be tasked with exploring betterment opportunities and supporting the development of minimum standards for cyber resilience. For example, if a data centre is destroyed in a cyber-attack, it should be rebuilt with a greater resilience to future attacks. For this to occur, the cost of upgrading the asset should be incorporated into the replacement cost. Furthermore, minimum standards for cyber resilience – similar to existing building codes – would improve cyber resilience of physical assets nationally.

In expanding the Scheme, international reinsurance pools that cover physical damage from cyber serve as a precedent for effective structure and administration.

5. Are there any changes in the governance, administration and resourcing of the terrorism reinsurance pool or the Terrorism Insurance Act that should be amended in light of potential interactions with the proposed cyclone and related-flood damage reinsurance pool?

The ICA considers the design of the Scheme appropriate for its current and expanded purpose. In respect to the ARPC's administration of both the terrorism and cyclone pools, ICA considers critical functions should be segregated to safeguard financial integrity of each pool. That said, this must be weighed against operational efficiency and unnecessary administration costs that can arise through duplication of resources. The ICA will continue to work with Treasury and the ARPC to support the implementation the cyclone pool.

As with the triennial review of the Scheme, the cyclone reinsurance pool should also undergo regular review in respect to its ongoing need.

If you would like to discuss this submission in further detail, please contact Kylie Macfarlane, the ICA's Chief Operations Officer, on 0418 111 154 or via email at kmacfarlane@insurancecouncil.com.au.

Regards

Andrew Hall
CEO and Managing Director