



Australian Government

The Treasury

Terrorism Insurance Act

Review

December 2021



© Commonwealth of Australia 2021

This publication is available for your use under a [Creative Commons Attribution 3.0 Australia](https://creativecommons.org/licenses/by/3.0/au/legalcode) licence, with the exception of the Commonwealth Coat of Arms, the Treasury logo, photographs, images, signatures and where otherwise stated. The full licence terms are available from <http://creativecommons.org/licenses/by/3.0/au/legalcode>.



Use of Treasury material under a [Creative Commons Attribution 3.0 Australia](https://creativecommons.org/licenses/by/3.0/au/legalcode) licence requires you to attribute the work (but not in any way that suggests that the Treasury endorses you or your use of the work).

Treasury material used 'as supplied'.

Provided you have not modified or transformed Treasury material in any way including, for example, by changing the Treasury text; calculating percentage changes; graphing or charting data; or deriving new statistics from published Treasury statistics — then Treasury prefers the following attribution:

Source: The Australian Government the Treasury.

Derivative material

If you have modified or transformed Treasury material, or derived new material from those of the Treasury in any way, then Treasury prefers the following attribution:

Based on The Australian Government the Treasury data.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are set out on the Department of the Prime Minister and Cabinet website (see www.pmc.gov.au/government/commonwealth-coat-arms).

Other uses

Enquiries regarding this licence and any other use of this document are welcome at:

Manager
Media and Speeches Unit
The Treasury
Langton Crescent
Parkes ACT 2600
Email: media@treasury.gov.au

Contents

- Contentsii**
- Executive Summaryiii**
- Recommendations and findingsiv**
- Chapter 1: Introduction1**
 - Recent developments.....1
 - Cyclone reinsurance pool1
 - Cyber terrorism resulting in property damage1
 - Scheme coverage and operating model.....2
 - Scheme eligibility2
 - When can a claim on the scheme be made?2
 - How a claim is funded3
- Chapter 2: Continuation of the Act.....5**
 - Assessment.....5
 - Private market capacity.....5
 - Conclusion6
- Chapter 3: Cyber-terror attacks that cause physical property damage.....7**
 - Cyber7
 - Cyber insurance market trends7
 - Risk mitigation8
 - Risk of cyber terrorism causing physical property damage9
 - Defining a cyber terror incident10
 - Operations and pricing.....10
 - Impact on broader insurance markets.....10
 - Conclusion11
- Chapter 4: Interactions between the terrorism pool and the proposed Cyclone reinsurance pool ..12**
 - ARPC Board background.....12
 - ARPC administration and resourcing.....13
 - Board skills assessment.....13
 - New skill requirements13
 - Increased demands on the Board14
 - Implementation of Cyclone Pool.....15
 - Interval between reviews.....15
 - Conclusion16
- Appendix A: Terms of Reference17**

Executive Summary

The Australian Government established the Terrorism Insurance Scheme (the scheme) on 1 July 2003 under The *Terrorism Insurance Act 2003*.

The scheme was introduced to alleviate the market failure, which occurred following the terrorist attacks in the United States on September 11, 2001 that resulted in global reinsurers refusing to underwrite commercial property damage caused by acts of terror.

The scheme is administered by the Australian Reinsurance Pool Corporation (ARPC), a public financial corporation operating with Government capital and backed by a \$10 billion Commonwealth guarantee. The Minister responsible for the Act is required to prepare a report every three years reviewing whether the scheme should continue. All previous reviews recommended the Act remain in force.

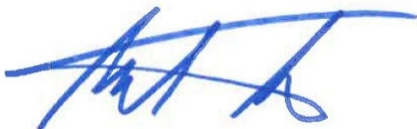
The 2021 Triennial Review (the Review) recommends that the scheme remain in place.

In the absence of the Act there would likely be a market failure in the terrorism insurance market with wider economic implications. The estimated global commercial market capacity available for Australian terrorism reinsurance is considered short of the level required to cover against large, but possible, terrorism incidents. Furthermore, industry stakeholders, including reinsurers and brokers indicated they would find it difficult to participate in the Australian terrorism insurance market without a mechanism like the ARPC.

This Review also considered whether the scope of the scheme should be expanded to include coverage for cyber terror attacks that result in physical property damage. The Review finds that cyber terrorism is an emerging risk and there is yet to be a clear and evident market failure in relation to physical property damage from cyber terrorism requiring government provision of reinsurance through the ARPC at this time.

Lastly, this Review also considered whether the ARPC Governance arrangements remain appropriate and found that the current arrangements remain appropriate for its existing functions.

The Terms of Reference for the Review were released on 2 July 2021 (Appendix A).



The Hon Michael Sukkar MP
Assistant Treasurer, Minister for Housing, Minister for Homelessness, Social and Community Housing

Recommendations and findings

Chapter 2: Continuation of the Act

Issue: Whether there continues to be a need for the Act.

Finding 1: In the ARPC's absence, a market failure in terrorism insurance markets covering physical property would likely re-emerge.

Recommendation 1: That the Act remains in force.

Chapter 3: Cyber-terror attacks that cause physical property damage

Issue: Whether cyber terrorism causing physical property damage should be included in the scheme.

Finding 2: Cyber insurance is an evolving market and there is yet to be a clear and evident market failure in relation to physical property damage from cyber terrorism.

Recommendation 2: That the Act maintains its current 'computer-crime' exclusion.

Chapter 4: Interactions between the Terrorism pool and the proposed Cyclone reinsurance pool

Issue: Whether the ARPC Board governance arrangements remain appropriate.

Finding 3: The current Board size remains appropriate for the ARPC's existing responsibilities. If the proposed cyclone reinsurance pool is implemented, the ARPC Board will require additional resourcing to ensure that it can provide sufficient scrutiny.

Recommendation 3 If the proposed cyclone pool is implemented:

- **3.1** The Government should ensure that ARPC's Board is appropriately resourced, including consideration of an expansion in the Board's size and/or increases in the time commitments of Board members.
- **3.2** The Government should appoint a new Board member(s) who is experienced with the insurance pressures facing residents of cyclone-prone areas.
- **3.3** The Government should appoint two board observers, one from APRA and one from the Commonwealth (such as the Australian Government Actuary), on a temporary basis, to help ensure a smooth implementation of the cyclone scheme.

Issue: Whether the ARPC remains adequately resourced and administered.

Finding 4: The ARPC is appropriately resourced to administer the terrorism pool and is taking steps to ensure it is ready to administer the new cyclone pool should it be confirmed. However, given the substantial change in functions, a review of the ongoing administration and resourcing of the ARPC may be necessary after the proposed new pool is operational.

Recommendation 4: If the proposed cyclone pool is implemented, a review of the ARPC's governance arrangements should be undertaken once their new governance arrangements are in place and the cyclone pool is in operation.

Issue: Whether the interval between TIA reviews remains appropriate

Finding 5: The TIA Review is a statutory requirement for the Government to assess whether there remains a continuing market failure in the private market for terrorism insurance. However, significant improvements in this market are unlikely to occur within the current review interval.

Recommendation 5: The interval between reviews of the Scheme should be expanded from three years to five years.

Chapter 1: Introduction

The Australian Government established the Terrorism Insurance Scheme (the scheme) under the *Terrorism Insurance Act 2003* (the Act) in response to the impact of terrorism events in the United States on September 11, 2001. These attacks caused significant commercial property losses, with corresponding large insurance payouts. Consequently, global reinsurers refused to underwrite for loss or damage to commercial property caused by terrorist activity, leaving commercial property owners to assume the risk of loss or damage to their properties.

The scheme provides terrorism insurance coverage for commercial property and associated business interruption losses and public liability claims. The scheme commenced on 1 July 2003 and is administered by the Australian Reinsurance Pool Corporation (ARPC).

The Act is intended to be a temporary measure to allow the re-emergence of an adequate private reinsurance market for terrorism risk. As such, there is a statutory requirement that the Act is subject to triennial reviews to determine whether there is an ongoing need for the scheme. This triennial Review covers the following issues:

- whether there continues to be market failure in the private sector supply of terrorism insurance, and consequently whether there is a need for the Act to continue;
- whether the risk of cyber terrorism causing physical property damage should be included in the scheme; and
- whether the governance, administration and resourcing of the scheme remain appropriate, including interactions between the Cyclone Reinsurance Pool and the Terrorism Reinsurance Pool.

Recent developments

Cyclone reinsurance pool

On 4 May 2021, the Australian Government announced that it intends to establish a reinsurance pool covering the risk of property damage caused by cyclones and cyclone-related flood damage. The pool would seek to improve the accessibility of insurance for households and small businesses mainly located in northern Australia. The ARPC would administer the pool, which is intended to commence on 1 July 2022.

The Reinsurance Pool Taskforce is considering the key design features of the reinsurance pool and how this function will link to the ARPC's terrorism reinsurance pool operations.

Cyber terrorism resulting in property damage

The 2018 Review considered the issue of whether to include cyber terrorism causing damage to property in the scheme. At the time, it found that there was no evident market failure for cyber terrorism insurance in relation to physical property damage. In support of that finding, it found that the underlying risk was considered low and that terrorist groups lack the technical sophistication to threaten Australia's security using cyber means at this time. It also noted that cyber insurance was a rapidly emerging sector of the Australian commercial insurance market, with coverage increasingly incorporated into business insurance packages or sold as an individual product.

Scheme coverage and operating model

Scheme eligibility

The Act operates by overriding terrorism exclusion clauses in eligible insurance contracts¹. An eligible insurance contract is a contract that provides insurance coverage for:

- loss of, or damage to, eligible property owned by the insured;
- business interruption and consequential loss arising from loss of, or damage to, eligible property that is owned or occupied by the insured or an inability to use all or part of such property; or
- liability of the insured that arises from the insured being the owner or occupier of eligible property.²

Further, the Act defines 'eligible property' as the following property located in Australia:

- buildings (including fixtures) or other structures or works on, in or under land;
- tangible property that is located in, or on, such property; and
- property prescribed by regulation.³

In practice, this means that insurers have an obligation to insure for the risk of terrorism, which encourages them to seek reinsurance. Reinsurance is available through the ARPC; insurers may choose to reinsure through the scheme, through the private reinsurance market, or retain the risk to their own balance sheet.

Schedule 1 of the *Terrorism Insurance Regulations 2003* (the Regulations) sets out a number of exclusions to the definition of an 'eligible insurance contract', including a contract for insurance that provides cover for destruction or damage to a 'mainly residential building'.⁴ Accordingly, the Act primarily applies to commercial property, however, following a recommendation in the 2015 Triennial Review, the scheme was extended to insurance cover for mixed-use and high value buildings.⁵

Schedule 1 also provides that a contract of insurance to the extent that it provides cover for loss arising from computer crime is not an eligible insurance contract for the purpose of s7(2) of the Act.⁶ The scheme does not provide cover for personal injury or death caused by a terrorist incident.

When can a claim on the scheme be made?

A claim on the scheme may be made for eligible terrorism losses arising from any declared terrorist incident covered by an eligible insurance contract where the insurer has a reinsurance agreement

¹ *Terrorism Insurance Act 2003* (Cth), s8(1).

² *Terrorism Insurance Act 2003* (Cth), s7(1).

³ *Terrorism Insurance Act 2003* (Cth), s3(definition).

⁴ *Terrorism Insurance Regulations 2003* (Cth), r 5.1.

⁵ The Treasury 2015, 'Terrorism Insurance Act Review: 2015', recommendation 9, page 25.

⁶ *Terrorism Insurance Regulations 2003* (Cth), r 5.32.

with the ARPC. The scheme will not be triggered unless the Minister who has administrative responsibility for the Act declares that a terrorist incident has occurred for the purpose of the Act.⁷

There has been one declared terrorist incident in the history of the scheme with 92 claims recorded as a result of the Lindt Café siege, totalling \$2.3 million from 20 insurers. As such, there has been no call on the Commonwealth guarantee (outlined below) in the history of the scheme.

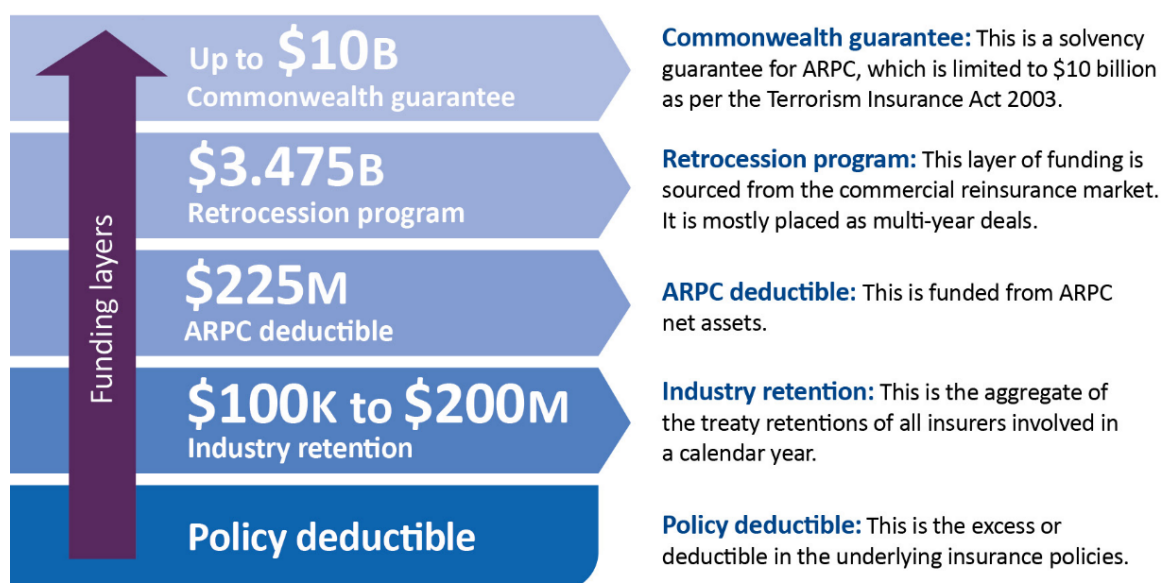
Further, claims may only be made for 'eligible terrorism losses'. 'Eligible terrorism losses' are losses or liabilities arising out of a declared terrorist incident that are not losses or liabilities arising from the hazardous properties (including radioactive, toxic or explosive properties) of nuclear fuel, nuclear material or nuclear waste⁸.

How a claim is funded

In the event of a declared terrorist incident for the purposes of the Act, claims would progress along the following sequence (Figure 1.1):

- a) Losses would be met first by industry up to the level of each insurer's retention; then
- b) From the ARPC capital up to the value of the deductible on the retrocession cover; then
- c) From the retrocession program (with any ARPC co-contribution being made from the ARPC capital and then through the Commonwealth guarantee) and finally;
- d) Through the Commonwealth guarantee, up to the \$10 billion cap.

FIGURE 1.1: ARPC FUNDING LAYERS



Source: ARPC, as of 01 January 2021⁹

The sum of these tiers represents the maximum claimable amount under the scheme. Should the total claimed losses exceed the capital of the ARPC, the value of retrocession cover purchased and

⁷ *Terrorism Insurance Act 2003* (Cth), s6.

⁸ *Terrorism Insurance Act 2003* (Cth), s3 (definition).

⁹ ARPC 2021, 'Annual Report 2019-20', p.5

the \$10 billion Commonwealth guarantee, a 'reduction percentage' would be applied and claims would be paid on a pro rata basis.¹⁰

Insurers that reinsure their terrorism risks with the ARPC retain part of the cost from a terrorist incident. The retention, similar to an excess or deductible, requires the insurer to pay the first part of any claim. Retentions for individual insurers are calculated as 5 per cent of fire and industrial special risk premiums collected by the insurer, with a minimum retention of \$100,000 and a maximum retention of \$12.5 million.¹¹

The ARPC's reinsurance agreement also provides for a maximum industry wide retention of \$200 million. If the sum of the retentions of maximum individual insurers in respect of all eligible terrorism losses caused by a single terrorist incident exceeds the maximum industry wide retention of \$200 million, then each insurer's retention is reduced proportionately.¹²

¹⁰ ARPC 2021, 'Annual Report 2019-20', p. 37

¹¹ ARPC 2021, 'Annual Report 2019-20', p. 12

¹² ARPC 2021, 'Annual Report 2019-20', p. 40

Chapter 2: Continuation of the Act

Issue: Whether there continues to be a need for the Act.

Finding 1: In the ARPC's absence, a market failure in terrorism insurance markets covering physical property would likely re-emerge.

Recommendation 1: That the Act remains in force.

Assessment

Risk of terror

The current National Terrorism Threat Level in Australia is 'Probable'. Individuals and groups continue to possess the intent and capability to conduct a terrorist attack in Australia. Densely populated cities such as Sydney and Melbourne remain the most exposed to a terrorist attack.

Terrorists continue to plot attacks in Australia. For example, over the last year, there were two religiously motivated terrorist attacks in Australia with arrests made in November 2020 and February 2021 on charges of planning for or preparing a terrorist attack.¹³

Furthermore, major industry stakeholders consulted in this Review consistently ranked terrorism highly in their risk management frameworks. Stakeholders indicated that while large scale terror events were rare, the potential of a large-scale terror loss in the absence of the scheme, would be financially detrimental.

Private market capacity

This Review finds that there would likely be market failure in the absence of the Act and thus recommends that the Act continue. While it is difficult to directly observe market failure given the presence of the ARPC and the \$10 billion Commonwealth guarantee, there are signposts pointing to likely market failure in its absence.

There continues to be a shortage of private market capacity for terrorism insurance. Through our consultation with reinsurers and brokers, we assess that there has not been significant change in global commercial market capacity for Australian terrorism reinsurance since the 2018 Review, which estimated capacity at approximately \$4 billion.¹⁴ The vast majority of this capacity (\$3.475 billion)¹⁵ is deployed into the Australian market through the ARPC's retrocession program. Industry stakeholders indicated that the scarce terrorism cover available outside the ARPC is often commercially unaffordable.

This private sector capacity remains significantly below the level of cover required to insure against large, but possible, terrorism incidents. ARPC modelling suggests that financial losses from a probable maximum single event loss from a conventional blast—an event which the Act was

¹³ Burgess, M 2021, 'DIRECTOR-GENERAL'S ANNUAL THREAT ASSESSMENT 2021 ASIO', viewed 26 August 2021 <<https://www.asio.gov.au/publications/speeches-and-statements/director-generals-annual-threat-assessment-2021.html>>

¹⁴ The Treasury 2018, 'Terrorism Insurance Act Review: 2018', chapter 2, page 4.

¹⁵ ARPC 2021, 'ARPC's retrocession program builds terrorism scheme's capital strength and helps cover the economy against terrorist attacks', viewed 23 August 2021 <<https://arpc.gov.au/2021/02/19/arpcs-retrocession-program-builds-terrorism-schemes-capital-strength-and-helps-cover-the-economy-against-terrorist-attacks/>>

designed to protect against—significantly exceeds this capacity**Error! Bookmark not defined.. Error! Bookmark not defined.**

There are also several reasons to believe private sector capacity would fall further in the absence of the ARPC:

- Terrorism risk is not easily understood by the market. Terrorism incidents are not random events, with both the likelihood and scale of loss events depending on the activity of terrorist groups and government counterterrorism capabilities. This information is not generally available to insurers.
- For the purposes of underwriting insurance products, there continues to be considerable uncertainty in determining what an actuarially sound price for terrorism risk would be. This is particularly an issue because there is a lack of depth in claims history.
- The ARPC has been in a position to help the market gain insight into exposure and risk through the security agencies. As a 'centre of expertise', a number of reinsurers noted that the ARPC's analytical work has improved their understanding of Australian terrorism risks. This has enabled the ARPC to bring in private market capacity through the ARPC's retrocession program.
- A number of reinsurers indicated that they would find it difficult to participate in the Australian terrorism insurance market without a mechanism like the ARPC. They noted that the ARPC is an efficient mechanism to pool terrorism risks and without its existence it would be very difficult to otherwise affordably insure the sum of properties in the ARPC portfolio (\$3.6 trillion) for terrorism risks.

Conclusion

This Review supports the continuation of the scheme.

At this time, there is no viable alternative for insurers to seek terrorism reinsurance cover at commercially reasonable prices. This Review finds that without the scheme, a market failure for terrorism insurance would likely re-emerge that would have significant negative impacts on economic activity. Most stakeholders who engaged in the Review's consultation process supported the continuation of the Act.

This recommendation aligns with previous reviews and with policy outcomes in international jurisdictions, with Governments continuing to support terrorism pools or government-backed reinsurance schemes. There are around 20 foreign jurisdictions with terrorism pools or reinsurance schemes¹⁶. Existing schemes that are subject to periodic reviews continue to be renewed. For example, the *Terrorism Risk Insurance Act* in the United States, which was set up in 2002 and is subject to periodic reauthorisation in order to continue, has been extended in 2005, 2007, 2015 and most recently in 2019 until 2027.

¹⁶ ARPC 2021, 'Annual Report 2019-20', p. 45

Chapter 3: Cyber-terror attacks that cause physical property damage

Issue: Whether cyber terrorism causing damage to physical property should be included in the scheme.

Finding 2: Cyber insurance is an evolving market and there is yet to be a clear and evident market failure in relation to physical property damage from cyber terrorism.

Recommendation 2: That the Act maintains its current ‘computer crime’ exclusion.

Cyber

Australia’s growing adoption of digital technology has produced an interconnected and technologically dependent society, which enjoys both a high quality of life and a resilient economy. This process has only accelerated since the beginning of the COVID-19 pandemic, where much of Australia’s workforce transitioned to remote working arrangements.

However, while digitisation has created opportunities, it is not without risks. The integration of information technology has increased businesses’ exposure to cyber-attacks. These attacks can vary from data theft, ransomware that renders computers inoperable, or even attacks that result in physical property damage. The capabilities and motives of cyber-attackers also vary, from sophisticated state-sponsored attacks, to financially motivated cyber criminals using ransomware, to terrorist groups that typically employ basic cyber methods.

In recent years, businesses and individuals have become increasingly aware of this risk, and in response, markets are developing solutions to help customers manage these risks, primarily through cyber security measures and to a lesser extent, cyber insurance.

In this Review, Treasury has considered the inclusion of cyber terror attacks that cause physical property damage within the scheme. This assessment has taken into account that cyber terror causing physical property damage is only a small portion of cyber risk broadly.

Cyber insurance market trends

The Cyber insurance market is an emerging and rapidly evolving market. While in Australia the cyber market is small compared to other insurance markets, estimated at approximately \$110 million in premiums in 2021¹⁷, it is growing. Marsh client data reveals that the number of Australian cyber insurance policies grew by almost 20 per cent in 2020 compared to the previous year.¹⁸

¹⁷ Parrant, M (Aon) 2021, ‘Cyber Insurance Market Insights – Q1 2021’, viewed 3 September 2021, <<https://aoninsights.com.au/wp-content/uploads/Cyber-Insurance-Market-Insights-Q1-2021-Final.pdf>>

¹⁸ Marsh 2021, ‘Cyber Insurance Market Recap 2020’, pg. 2

In recent years cyber insurers have experienced a marked rise in the severity of cyber insurance claims, with direct loss ratios (the proportion of insurer income paid to claimants) jumping from 47 per cent to 73 per cent between 2019 and 2020.¹⁹

However, insurers have not responded with a broad-based withdrawal in market capacity. Instead, insurers and reinsurers are adjusting their practices to ensure more sustainable underwriting practices. Insurers are also reevaluating the scale and frequency of cyber claims in response to poor claims results; and accordingly, premiums grew 51 per cent in 2020.¹⁸

This process has also included efforts to provide improved clarity to policyholders. Up until recently, most cyber insurance coverage was non-affirmative. This means that generalised clauses in non-cyber specific policies (such as a property insurance contract), would likely have covered cyber-related losses. “Silent cyber” as this type of cover is known, created significant ambiguity on which types of cyber incidents were covered and if they were even intended to be covered at all. Concerned by this ambiguity and its consequence for insurer solvency, the industry, led by Lloyd’s of London, has taken steps to remove silent cyber from their policies. Today most renewals either expressly include cyber cover or expressly exclude cyber exposures.

Similarly, because of clarifying cyber coverage, some insurers and reinsurers have identified cyber-attacks causing physical property as an unintended risk. As such, many insurers have moved to exclude property damage from their standalone cyber offerings.

Improved awareness of cyber risk is spurring more stringent underwriting practices. Insurers increasingly assess business exposure to cyber losses (i.e. scale and dependence on IT infrastructure) as well as the cyber mitigation strategies businesses employ, such as cyber security software and staff training on cyber safety protocols.

Insurers are also reassessing the nature of cyber risk in their portfolios, with many insurers now considering cyber as a systemic risk that is difficult to insure. The modern economy runs on interconnected information technology infrastructure, which is not delimited by geography. Consequently, reinsurers are concerned about potentially widespread claims over short periods of time, similar to how insurers were exposed to business interruption losses from the COVID-19 pandemic. To manage this accumulation risk, insurers are actively capping limits on individual risks.

Risk mitigation

The Government and private businesses are proactively taking measures to mitigate the risk of cyber-attacks.

Over the last decade a substantial cyber security industry has developed in Australia, with cyber security spending now amounting to approximately \$5.6billion Australia wide, with 10 per cent²⁰ growth in 2020 alone, a sum which dwarfs the size of the Australian cyber insurance market (approximately \$110 million). Stakeholders consulted as part of this Review, also shared that their cyber resilience strategies extended to their internal procedures, which included cyber safety checks, training and attention from corporate boards.

¹⁹Fitch Ratings 2021, ‘Sharply Rising Cyber Insurance Claims Signal Further Risk Challenges’, April 2021, viewed 1 September 2021, <<https://www.fitchratings.com/research/insurance/sharply-rising-cyber-insurance-claims-signal-further-risk-challenges-15-04-2021>>

²⁰AustCyber 2020, ‘Australia’s Cyber Security Sector Competitiveness Plan 2020’, viewed 1 September <<https://www.austcyber.com/resources/sector-competitiveness-plan/chapter1>>

The government and regulators are focusing greater efforts on the cyber security of Australian businesses. These efforts include:

- In July 2019, APRA introduced Prudential Standard CPS 234, which aims to minimise the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets, including information assets managed by related parties or third parties.²¹
- In September 2020, the Government introduced a voluntary code of practice for smart product manufacturers. The Code of Practice contains thirteen principles that signal Government expectations to manufacturers about the security of smart products.²²
- In late 2020, changes to the *Security of Critical Infrastructure Act 2018* were introduced into parliament, which aim to strengthen the security of Australia's infrastructure through positive cyber security obligations.²³
- In 2020, the Government commenced a review of the *Privacy Act 1988*. This aims to bring Australia's privacy laws into the digital era, strengthen privacy protections for individuals and streamline compliance for businesses working across international borders.²⁴
- In July 2021, the Government opened consultation on options for regulatory reforms and voluntary incentives to strengthen the cyber security of Australia's digital economy.²⁵

Risk of cyber terrorism causing physical property damage

The Australian Cyber Security Strategy notes that while terrorist groups and extremists are effective at using the internet to communicate and generate attention, they generally employ very basic cyber techniques and capabilities such as distributed denial of service (DDoS) activities, hijacking social media accounts and defacing websites. These groups currently pose a relatively low cyber threat, particularly a low threat of the kind of technically sophisticated cyber-attack that would typically be required to cause major physical property damage.²⁶

Stakeholders consulted during this Review, frequently raised that cyber-threats such as data theft and ransomware presented far greater risks to their businesses than those posed by cyber terror attacks causing physical property damage. This feedback appears to be supported by industry research:

- A CrowdStrike survey conducted of 200 senior IT decision-makers and security professionals across Australia's major industry sectors, found that two thirds had suffered a ransomware attack in the 12-month period to November 2020, of which one third paid the ransom.²⁷
- An IBM report released this year found that the average time to detect and contain a data breach over the past year was 287 days, and in Australia data breaches cost companies an average of \$2.82 million (\$USD) per incident.²⁸

²¹Australian Prudential Regulatory Authority 2019, 'CPS 234', July 2019

²²Department of Home Affairs 2021, 'Voluntary Code of Practice', viewed 2 September 2021, <<https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice>>

²³Australian Parliament House 2020, viewed 10 September 2021

<<https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fbillhome%2Fr6657%22>>

²⁴Attorney General's Department 2020, 'Privacy Act Review Issues Paper', October 2020

²⁵Home Affairs 2021, 'Strengthening Australia's cybersecurity regulations and incentives', July 2021

²⁶Home Affairs 2020, 'Cyber Security Strategy 2020', pg.13, August 2020

²⁷Purtell, J (Australian Broadcasting Corporation), 'Australian organisations are quietly paying hackers millions in a 'tsunami of cyber crime'', viewed 1 September 2021, <<https://www.abc.net.au/news/science/2021-07-16/australian-organisations-paying-millions-ransomware-hackers/100291542>>

²⁸IBM 2021, 'Data Breach Report 2021', July 2021

Consequently, this Review finds that while cyber terror causing physical property damage does pose a risk to Australian businesses, it is not the main driver of cyber-related financial losses, nor is it the main motivator for businesses pursuing cyber risk mitigation strategies.

Expanding the terror scheme

While some stakeholders, including those representing business policyholders, supported the inclusion of cyber terrorism causing physical damage, others highlighted a number of concerns in operating such a scheme.

Defining a cyber terror incident

There are practical difficulties with providing cyber cover through the scheme purely for ‘terrorism’. Stakeholders noted that it is most likely that cyber incidents will be motivated by malicious motives other than terrorism. As incidents tend to emanate from overseas, the culprits and their intent could be difficult to determine. If the scheme were to be extended to cover cyber terrorism, this could lead to uncertainty as to whether the ARPC would be liable in the event of an attack. This could place pressure on the Government to respond even when an incident may not be a terrorism incident.

Operations and pricing

Some stakeholders noted that the ARPC’s current premium structure, which is based on postcodes and urban density, would be inappropriate if the scheme were broadened to cover cyber events. This is because cyber risk to physical property would likely have a different geographic and industry profile to the existing terrorism scheme.

Impact on broader insurance markets

Several stakeholders noted that extending the scheme to include cyber terrorism risk causing physical property damage could have a number of potential impacts on the broader insurance and reinsurance market.

Some of these could adversely impact the function of the current scheme and private markets:

- Stakeholders indicated that including cyber risk in the ARPC’s reinsurance scheme would reduce the already limited appetite for Australian terrorism risk through the ARPC’s retrocession program. This feedback aligns with the inclusion of chemical and biological attacks in the ARPC’s terrorism scheme in 2015, which reduced private sector demand for the ARPC’s retrocession program.²⁹
- As noted in the 2018 Review, cyber insurers could be crowded out if the scheme were broadened, as they would not be able to compete against a government-backed scheme. Some also feared that if the scheme were extended to provide cover only for property damage from cyber terrorism, and if the direct insurer did not already provide cover for all losses arising from a cyber incident (‘all-risks’), the direct insurer would be under pressure to offer the ‘all-risks’ part of the cover—even if they did not have the capacity to do so.

Whereas others were more positive:

- Stakeholders argued the ARPC could perform a role as a ‘centre of expertise’, similar to its existing terrorism program. By leveraging the ARPC’s access to Australia’s security agencies, it could provide analytical work that improves market understanding of Australian cyber terrorism risks.

²⁹ Finity 2018, ‘2018 Review of Terrorism Insurance’, p. 10.

This may improve the market's assessment of risk and pricing, and hence support commercial appetite.

- Some also speculated that the ARPC's unique ability to pool risks, could potentially create an attractive retrocession product. However, they noted that this would require further investigation.

However, most stakeholders stressed that the inclusion of cyber in the terrorism scheme would be a substantial intervention at a time when the ARPC is undergoing significant change. As noted above, cyber risks are a fundamentally different risk to those covered by the existing terrorism scheme and hence would require significant increases in the ARPC's capability to ensure the risk was appropriately priced and modelled. Accordingly, these stakeholders argued that given the ongoing implementation of the cyclone and related flooding reinsurance pool (cyclone pool), another substantial intervention could disrupt the ARPC's ability to carry out its other functions.

Conclusion

The cyber insurance market is still nascent, with a limited capacity to underwrite cyber risks, including cyber terrorism risks causing physical property damage. However, in emerging financial markets it is not uncommon for there to be gaps. New risks not previously contemplated often fall between existing classes of commercial insurance products. Since the last Review in 2018, the industry has proactively sought to clarify and develop cyber insurance products which are financially sustainable. In time, the cyber insurance market may mature to better understand risk and increase its capacity to provide insurance solutions to customers.

Furthermore, insurance is not a panacea and not all risks can or should be insured. Governments, businesses and individuals, both in Australia and internationally, are increasingly becoming aware of the need for mitigation-based solutions to cyber risks. Indeed, over time, these actions may even help foster insurer appetite to underwrite new risks.

This Review does not consider the current exclusion of computer crimes as producing a market failure that warrants intervention through the ARPC. However, there is potential for terrorist groups to develop greater capabilities in the longer term, which could change this assessment in a future review.

Chapter 4: Interactions between the terrorism pool and the proposed Cyclone reinsurance pool

The proposed cyclone pool will pose both challenges and opportunities for the ARPC. The Review closely considered the ARPC's strategic settings to ensure that they remain appropriate.

Issue: Whether the ARPC Board governance arrangements remain appropriate.

Finding 3: The current Board size remains appropriate for the ARPC's existing responsibilities. If the proposed cyclone reinsurance pool is implemented, the ARPC Board will require additional resourcing to ensure that it can provide sufficient scrutiny.

Recommendation 3 If the proposed cyclone pool is implemented:

- **3.1** The Government should ensure that ARPC's Board is appropriately resourced, including consideration of an expansion in the Board's size and/or increases in the time commitments of Board members.
- **3.2** The Government should appoint a new Board member(s) who is experienced with the insurance pressures facing residents of cyclone-prone areas.
- **3.3** The Government should appoint two board observers, one from APRA and one from the Commonwealth (such as the Australian Government Actuary), on a temporary basis, to help ensure a smooth implementation of the cyclone scheme.

Issue: Whether the ARPC remains adequately resourced and administered.

Finding 4: The ARPC is appropriately resourced to administer the terrorism pool and is taking steps to ensure it is ready to administer the new cyclone pool should it be confirmed. However, given the substantial change in functions, a review of the ongoing administration and resourcing of the ARPC may be necessary after the proposed new pool is operational.

Recommendation 4: If the proposed cyclone pool is implemented, a review of the ARPC's governance arrangements should be undertaken once their new governance arrangements are in place and the cyclone pool is in operation.

Issue: Whether the interval between TIA reviews remains appropriate

Finding 5: The TIA Review is a statutory requirement for the Government to assess whether there remains a continuing market failure in the private market for terrorism insurance. However, significant improvements in this market are unlikely to occur within the current review interval.

Recommendation 5: The interval between reviews of the Scheme should be expanded from three years to five years.

ARPC Board background

Under section 12 of the TI Act, the ARPC is required to have a Chair and at least four, but no more than six, part-time members on the Board. As of September 2021, the ARPC Board consisted of five

members, with one vacancy. In accordance with the ARPC Board Charter³⁰, the Board's responsibilities include:

- setting the strategic direction and financial objectives for the ARPC and monitoring their implementation;
- establishing and maintaining productive working relationships with the Treasury, the Minister's office and other relevant Commonwealth and State/Territory agencies, as appropriate;
- establishing and maintaining productive working relationships with key stakeholders within the terrorism insurance and reinsurance markets, and in particular, global terrorism reinsurers;
- determining that the ARPC has an appropriate risk management framework in place, determining in consultation with management the risk appetite and risk tolerance levels within which the ARPC should operate;
- monitoring compliance with regulatory requirements, ethical standards and external commitments, and the implementation of the ARPC policies and relevant Government policies; and
- appointing and reviewing the performance of the Chief Executive (CEO).

ARPC administration and resourcing

In the current context of terrorism risk, the governance, administration, and resourcing of the ARPC remains appropriate for the terrorism reinsurance scheme. In 2019, the Australian National Audit Office (ANAO) performance audit independently reviewed the terrorism reinsurance scheme. The ANAO reported that the ARPC operates effectively and enables Australian businesses to efficiently manage terrorism risk.³¹

The proposed new cyclone pool would demand significant increases in the resourcing and capabilities of the ARPC. Accordingly, the ARPC is progressing implementation work to ensure all the necessary people, systems, and processes are in place to commence the new pool from 1 July 2022, while maintaining the ongoing effective administration of the terrorism pool. This includes substantial upgrades in IT infrastructure, increased hiring, and liaising and supporting the Treasury-led Reinsurance Pool Taskforce.

The Review considers the ARPC is taking appropriate steps to ensure it is ready to administer the terrorism pool and implement the proposed new cyclone pool. However, given the substantial increase in functions, further resourcing and administration needs may become apparent once the scheme is in operation. Consequently, a review of the ongoing administration and resourcing of the ARPC may be necessary once the new pool is operational.

Board skills assessment

New skill requirements

To assess the ARPC Board's changing skill requirements should the Government confirm the proposed cyclone reinsurance pool a Board skill matrix has been developed in Table 1.1.

This Table shows that the current skill composition largely remains appropriate for the organisation's expected future needs. Indeed, some of the new desirable board skills: experience in organisational

³⁰ Australian Reinsurance Pool Corporation 2019, 'Board Charter', p. 4

³¹ Australian National Audit Office 2019, 'Management of the Terrorism Reinsurance Scheme', pg.8

change and catastrophe modelling, which are two key skill areas that will help the organisation adapt and operate the new reinsurance pool, are already well represented on the Board.

However, there is one area that the Board should add expertise in. Unlike the current terrorism pool, the cyclone pool is expected to pay substantial and more frequent claims. While as a reinsurer the ARPC will not handle claims at a policyholder level; it is the responsible entity for a significant intervention in the Australian reinsurance market, and there is strong community expectations and interest in the scheme.

To ensure the ARPC is appropriately equipped to engage with the community, it will need to introduce new processes and build up new stakeholder relationships. A Board member(s) that is familiar with the insurance pressures facing cyclone prone areas, including the drivers of premium affordability, insurance claims processes and mitigation; and who is also well placed to help foster stakeholder relationships, including with consumers, brokers and the insurance industry, would help ensure adequate oversight of these new functions.

Table 1.1 Board Skill requirements

Current Board requirements	
Skills	Presence on Board
Actuarial	✓
Audit	✓
Board experience	✓
Corporate governance	✓
Directors Duties	✓
Financial management / Accounting	✓
Insurance management	✓
Investments	✓
Leadership	✓
Legal	✓
Private sector	✓
Public sector	✓
Risk management	✓
Strategy	✓
New Board skill requirements	
Organisational change	✓
Catastrophe underwriting	✓
Community experience in cyclone prone areas	X

Increased demands on the Board

The ARPC's expanded functions will also require increased depth in certain skills and greater time commitments from Board members if the proposed cyclone pool is confirmed.

As a consequence of the expansion, the Board will experience increased workloads across its responsibilities, including its audit and compliance duties, assessing retrocession, oversight of the ARPC's investment portfolio, and overseeing the implementation and management of the cyclone pool.

Furthermore, there is enhanced significance of the Board's role in ensuring the sustainable operation of the ARPC. As noted above, the new cyclone pool is expected to have more frequent, and at times substantial claims that could be funded from the Government's guarantee. Consequently, Board oversight of the ARPC's operations, especially from a risk management perspective, will take on increased significance. Currently, the ARPC Board reviews a risk management statement at each Board meeting. This statement identifies four broad risk categories:

- insurance risk —which covers risks across underwriting, claims and actuarial disciplines;
- operational risk —covering risks arising from system failure or inadequacies, human error or external events;
- capital risk— which covers risks associated with the ARPC's ability to make claims; and
- financial risk — which covers risks associated with market fluctuations, credit risk and liquidity risk.

These risks will be significantly greater if the cyclone pool becomes operational.

Given these increased responsibilities, the ARPC board will require greater resources to fulfill its functions if the cyclone pool is confirmed. This could include increasing the time commitments of the existing board or by increasing the board's size.

Implementation of Cyclone Pool

Given the significant expansion of the ARPC's functions, it is important for both smooth transition from the pool's design to its implementation, and for Government visibility over the process. Accordingly, the Government should make two observer appointments on a temporary basis to the ARPC Board from APRA and the Commonwealth (such as from the Australian Government Actuary (AGA)).

This approach is consistent with the ARPC's establishment. During the initial set-up of the terrorism pool, two officials from the Treasury were appointed as part-time members for initial periods of six months. These appointees were responsible for drawing up the scheme and helped assist in the establishment of the Corporation.

It is also consistent with recent Government practice, with a number of Government Boards appointed from within Government on both temporary and ongoing bases. For example, a Treasury official was recently appointed as an observer to the National Housing Finance and Investment Corporation Board, which has improved Government/departmental oversight at a time of significant expansion to NHFIC's functions. Likewise, the Tuition Protection Board, has a number of permanent Government officials, including appointees from APRA and the AGA, which provide oversight from prudential and actuarial perspectives respectively.

Interval between reviews

When the Act was introduced in 2003, it was intended to be a temporary measure to allow the re-emergence of an adequate private reinsurance market for terrorism risk. As such, there is a statutory requirement that the Act is subject to triennial reviews to determine whether there is an ongoing need for the scheme.

However, all six reviews conducted since 2003 (including this one), have found that there remains an ongoing need for the Scheme to continue. Furthermore, as noted in Chapter 2, overseas jurisdictions are continuing to introduce terrorism insurance schemes, or choosing to extend existing schemes.

There are significant structural barriers to a private market re-emerging in Australia that could offer terrorism insurance at commercially reasonable prices (Chapter 2). For the purposes of the Act, any substantial growth in private market capacity, is likely to take significantly longer time than the current

interval between Reviews. Accordingly, the interval between reviews of the Scheme should be increased from three years to five years.

Conclusion

The incorporation of the new cyclone pool would increase demands on the ARPC Board. Given the significant increase in functions, the board must be sufficiently equipped to ensure the appropriate implementation and management of the cyclone pool.

The Government should ensure that ARPC's Board is appropriately resourced, including consideration of an expansion in the Board's size and/or increases in the time commitments of Board members. Furthermore, the Government should appoint temporary observers from APRA and the Commonwealth (such as the AGA) to ensure a smooth transition from the pool's design to its implementation.

The Government should also seek to appoint a Board member(s), who is familiar with the pressures facing residents of cyclone-prone areas, including knowledge of insurance premium affordability issues and the role of mitigation.

The current three-year interval between reviews of the TIA is too short and should be increased to five years. Substantial developments in the market for private terrorism insurance are unlikely to occur over a three-year time horizon.

Further implications for the ARPC's governance and administrative arrangements are dependent on the final design of the cyclone reinsurance pool, and the requisite skills, oversight and resourcing it demands.

Appendix A: Terms of Reference

The *Terrorism Insurance Act 2003* (the Act) established a scheme for replacement terrorism insurance coverage for commercial property and associated business interruption. The Act also established the Australian Reinsurance Pool Corporation (ARPC) as a statutory authority to administer the scheme. Both the scheme and the ARPC began operations on 1 July 2003.

The scheme was established as an interim measure to address a specific market failure in the private provision of terrorism insurance. The scheme is intended to operate only while terrorism cover is unavailable commercially on reasonable terms. As a result, s. 41 of the Act requires that: “At least once every three years after the start-up time, the Minister must prepare a report that reviews the need for this Act to continue in operation.”

Previous reviews were completed in 2006, 2009, 2012, 2015 and 2018. Each review concluded that the Act should continue in operation, subject to further review in no more than three years.

To allow for completion of the Review by 12 December 2021, Treasury will report to the Minister on:

- whether there continues to be market failure in the private sector supply of terrorism insurance, and consequently whether there is a need for the Act to continue;
- whether the governance, administration and resourcing of the scheme remain appropriate, including interactions between the Cyclone Reinsurance Pool and the Terrorism Reinsurance Pool; and
- whether the risk of cyber terrorism causing physical property damage should be included in the scheme.