NIBA
National Insurance Brokers Association.

30th July 2021

National Insurance Brokers Association of Australia

Submission to the Triennial Review of the Australian Reinsurance Pool Commission.

The National Insurance Brokers Association (NIBA) welcomes the opportunity to provides these comments in response to the Triennial Review of the Australian Reinsurance Pool Corporation (ARPC) on behalf of the intermediated insurance industry.

The ARPC was established to address gaps in the terrorism risk insurance market caused by the withdrawal of reinsurers following the September 11 terrorist attacks.

Since the establishment of the Scheme, a number of insurers and reinsurers have re-entered the market however, capacity remains limited. Based on the experiences of NIBA, it unlikely that the private market would be able to provide cover on the scale currently provided by the Scheme.

During the previous review, physical damage resulting from a cyber terrorist attack was identified as a gap in the cover provided by the Scheme. However, the report found that the risk of such an event occurring was low. Little has changed since the 2018 report to suggest that the risk has increased.

The Risk of Physical- Cyber Terrorist Attacks

There has only been a small number of real-life examples where a cyber-attack has resulted in physical damage. Of these, it is unlikely that any would meet the definition of a terrorist act under S100.1 of the *Criminal Code Act 1995*. This is primarily because the majority of examples were carried out by state-sponsored actors.

2000- A disgruntled job applicant, used stolen equipment to hack into the Maroochy Shire Council waste management system, causing the release of 800,000 litres of raw sewage into the environment.

2008- A teenager in Poland hacked the city's tram system with a homemade transmitter, causing the derailment of four trams and injuring a dozen people.

2008- An explosion occurred along a pipeline in Turkey. It was later found that hackers had increased the pressure of the oil flowing through the pipeline while also disabling the alarm system that would usually detect such an event.

2010- A computer worm, known as Stuxnet, targeted Iran's nuclear enrichment facilities. The worm caused significant damage to almost a quarter of the facility's centrifuges while simultaneously preventing the reporting of any damage to the control room.

2014- An unnamed steel mill in Germany was affected by a cyber-attack that disabled the ability to shut down a blast furnace, leading to significant physical damage.

2015- A cyber-attack against power distribution control centres in Ukraine led to approximately 30 substations being taken offline and a loss of power to more than 230 000 residents. A further attack on a control centre was reported the following year.

2017- Saudi Arabian oil refineries were targeted by a malware programme designed to attack safety systems. The attack caused a number of refinery processes to shut down.

Although these attacks have been rare, the rise of IoT makes attacks such as these increasingly attractive to malicious actors. It is predicted that 35 billion IoT devices will be installed around the world by the end of this year. While the number of connected devices has increased significantly over the past few years, levels of awareness and cyber security have not always kept pace. Last year, the Australian Cyber Security Centre conducted a survey among small and medium businesses (up to 199 employees), almost half rated their cyber security understanding as 'average' or 'below average' and had poor cyber security practices.

Availability of Cover for Physical-Cyber Attacks in the Commercial Market

A number of commercial insurers now include cover for physical damage and business interruption losses stemming from a cyber-attack as part of their standard property and casualty (P&C) policies.

However, many of these policies exclude acts of terrorism. Given the current low capacity within the commercial terrorism market, it is unlikely that cover for physical

damage resulting from a cyber terrorist attack would be able to be sourced from the commercial market.

It is NIBA's opinion that the Scheme is best placed to facilitate this cover.

International Approaches

Internationally, work has already been undertaken to provide coverage for these types of attacks. To assist Treasury with their review, NIBA has reached out to its counterparts in the World Federation of Insurance Intermediaries (WFII) who have provided the following information.

United Kingdom

In 2018, the UK's Pool Re was extended to include "*material damage and direct business interruption losses caused by acts of terrorism that are triggered by remote digital means using a cyber trigger*" This is termed 'remote digital interference' or RDI cover.

RDI is more restrictive than the general Pool Re cover, as it covers only resulting named perils in the policy (as opposed to the "all resulting risks" of terrorism coverage). Business interruption cover only applies to physical damage to the property and not to business interruption losses resulting from a loss of systems.

As a reinsurance provider, Pool Re only pays claims to insurers if losses were covered in the underlying policy. This means that although Pool Re may include coverage for physical-cyber terrorist attacks, insurers are not required to provide this option to their customers.

As with other coverages, "state sponsored" acts of terrorism are excluded.

France

In France, it is compulsory for insurers to provide coverage for terrorism in property and motor vehicle insurance policies.

The legal definition of terrorism specifically includes "computer offenses" and coverage under the terrorism reinsurance program Gestion de l'assurance et de la réassurance des risques attentats et actes de terrorisme (GAREAT) is based on whether an incident meets that legal definition.

Unlike other reinsurance programs GAREAT does not require a declaration of government for an event to be considered a terrorist attack.

As a result, physical damage and business interruption resulting from cyber-terrorism are eligible for coverage.

United States of America

In the United States, terrorism cover is provided by the Terrorism Risk Insurance Program (TRIP) under the Terrorism Risk Insurance Act (TRIA).

Cover is only available for incidents that are certified by the US Treasury Secretary, based on a number of conditions. TRIP is silent on whether coverage for cyber and other non-conventional terrorism risks were included however, this has since been clarified by the U.S Treasury who stated that cyber-terrorism is included under the TRIA

However, terrorism losses must be incurred by the insurer before TRIP co-insurance would be provided. This means that TRIP coverage is not available in the case of insurance policies that exclude cyber-attacks.

Since the announcement, insurers have generally excluded these events from property and casualty cover. Where cyber-attacks are covered under a property policy, TRIA requires that this extends to cyber-terrorism.

NIBA understands the United States Government Accountability Office is currently examining a number of issues surrounding cyber terrorism including the risks and costs of cyberattacks on U.S. critical infrastructure, insurance coverage that is available for losses related to cyber risk, including cyberterrorism and the extent to which TRIP, under the Terrorism Risk Insurance Act (TRIA), is structured to respond to cyberattacks and cyberterrorism.

Issues for the 2024 Triennial review

NIBA notes that the current triennial review process provides little scope to focus on other issues that affect the operation of the Scheme. NIBA proposes that a series of work be undertaken, building on the work undertaken by the University of Queensland.

A number of gaps were identified, that would be worthy of further investigation as to whether the Scheme needs to be modified to address these issues. There are many areas where the operation of the Scheme can be unpredictable. Given the serious nature of the risks covered by the Scheme, more work should do be done to ensure the Scheme responds as expected by policyholders.

In particular, NIBA recommends that work be undertaken to examine the relationship between the Scheme and existing motor vehicle, personal injury and commercial terrorism cover. The findings of this work should be used to inform the 2024 Triennial review and ensure the Scheme remains fit for purpose in the absence of adequate commercial capacity.

Please do not hesitate to contact me if you would like to discuss any aspect of this submission.

Dallas Booth
Chief Executive Officer
National Insurance Brokers Association

Email: dbooth@niba.com.au