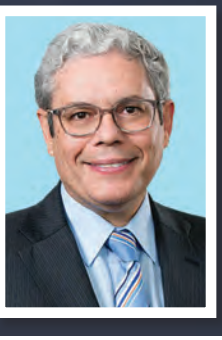
COUNTRY PROFILE – AUSTRALIA

Commercial property at risk from cyber attacks

Risk is ever evolving – and some new risks require serious research to put them into perspective. Australian Reinsurance Pool Corporation identified cyber terrorism causing physical damage to commercial property as an area requiring deep research and commissioned the Organisation for Economic Co-operation and Development and the Centre for Risk Studies at the Judge Business School, University of Cambridge, to provide insights into the threat in Australia. **ARPC**'s **Dr Christopher Wallace** walks us through this cutting-edge research.



Australian Reinsurance Pool Corporation (ARPC) manages the nation's terrorism reinsurance scheme – but the scheme currently excludes coverage for physical damage caused by cyber terrorism. Since this could cause systemic issues for the commercial real estate market in the event of an attack, ARPC decided to explore ways to understand this protection gap better.

Project scope

For Australia, the research study aimed to:

- Evaluate available insurance coverage for cyber attacks involving declared acts of war, criminality and/or terrorism
- Evaluate the practicalities of extending ARPC's insurance coverage to include cyber terrorism
- Evaluate relevant international experience in introducing coverage of cyber terrorism to terrorism insurance schemes
- Evaluate the direct and indirect impacts of insured and uninsured losses to commercial property and business interruption from acts of cyber terrorism
- Provide estimates for insurance losses and GDP economic impact
- Assess realistic cyber-attack scenarios including likelihood, direct/indirect impacts and existing insurance coverage, and
- Identify systemic or contagion risks from cyber risks to the economy.

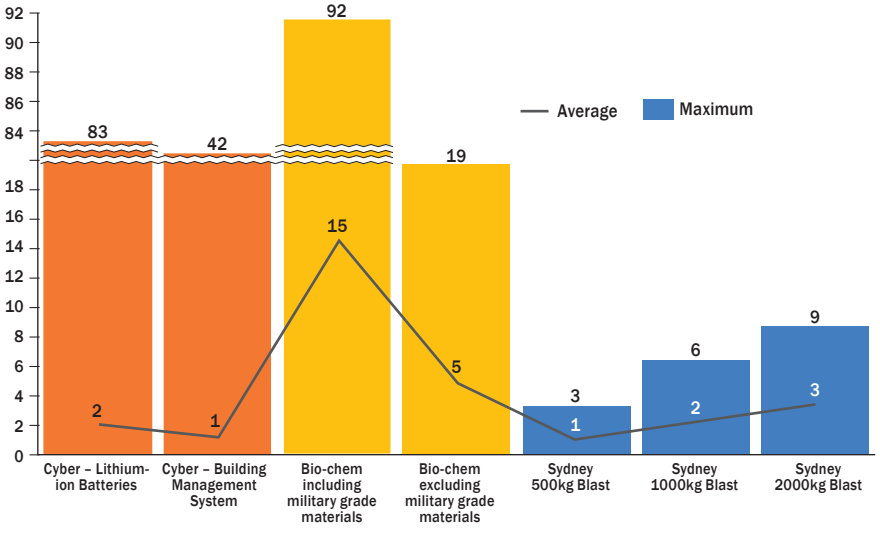
The work was split between the Organisation for Economic Co-operation and Development (OECD) and the Centre for Risk Studies at the Judge Business School, University of Cambridge (Cambridge). OECD addressed points one to three and Cambridge four to seven.

Wake-up call

In brief, cyber terrorism is not covered by commercial property insurance in Australia while the terrorism reinsurance scheme administered by ARPC excludes cover for cyber terrorism.

According to the two scenarios Cambridge modelled, average expected

Figure 1: Expected average and maximum scenario losses (A$bn)



losses are in line with those from a traditional explosive blast attack in the Sydney CBD and are within the capacity of the scheme while maximum losses exceed the capacity of the scheme. In either event, they are too substantial to be left uninsured.

Cyber cover doesn't cover property damage

Cyber insurance in Australia generally offers broad coverage for property damage but most policies have exclusions for war and terrorism and so exclude damage from cyber terrorism.

Most commercial property in Australia is reinsured by ARPC but for declared terrorism incidents, terrorism exclusions in underlying insurance policies are annulled. Insurers must pay claims to the extent the cover is for eligible insurance under the ARPC scheme - but as computer crimes are an excluded peril from the ARPC scheme, this would not be the case for cyber terrorism.

In short, since cyber is not an eligible peril under the ARPC scheme, the terrorism exclusion in the underlying policy would not be annulled and losses from a cyber-terrorism incident causing commercial property damage to would be largely uninsured.

ARPC and the government could find it difficult to explain why an incident declared as terrorism by the government is not reinsured by the government reinsurer which has a mission of supporting recovery and paying claims after a terrorism event

Extending the scheme to include cyber terrorism

Introducing cover to fill this gap is unlikely to occur without ARPC, and reinsurers involved in the study said their preferred method of involvement was assuming part of the aggregate risk through ARPC - although pricing methodology and coverage would still need to be determined.

ARPC's basis of purchasing retrocession would also need to be considered. For instance, is cyber cover added to the existing programme or should it be purchased as a separate programme?

Cyber-attack scenarios

Causing physical damage using cyber can be achieved through disrupting an embedded ignition source or source of kinetic energy that can be leveraged through digital systems.

Cambridge proposed the following energy source scenarios:

- Lithium-ion batteries
- Fuel for boilers
- Machinery energy
- Hazardous materials
- Aircraft in flight
- Remotely-powered vehicles
- Widespread flooding
- Power outage

Cambridge explored two possible scenarios that would impact the ARPC portfolio and the Australian economy: A lithium battery fire and a building management system (BMS) attack. For each scenario Cambridge posited three outcomes: S1 (some damage to property), S2 (more extensive damage to property), X1 (most damage to property).

Table 1: Lithium battery fire systematic attack scenario expected economic loss estimates (in A$m)

	GDP@Risk	ARPC Total Insured Loss (Average)	ARPC Total Insured Loss (Maximum)
S1	$21,213	$2,027	$83,314
S2	$39,337		
X1	$74,349		

Table 2: BMS targeted attack scenario expected economic loss estimates (in A$m)

	GDP@Risk	ARPC Total Insured Loss (Average)	ARPC Total Insured Loss (Maximum)
S1	$13,048	$1,304	$41,832
S2	$26,007		
X1	$60,186		

Source: Cambridge Centre for Risk Studies

Lithium battery fire systematic attack scenario

This scenario involves the 'weaponisation' of personal technology with fires caused by a thermal runaway reaction and sees a terrorist cell target a vulnerability with some laptops to cause a thermal runaway. The terrorist cell initiates the attack at night causing batteries that are charging to overheat and catch fire.

Local emergency services are overwhelmed with fires in many locations and need to prioritise hospitals and large buildings. The result is that whole floors of large commercial buildings are destroyed, some smaller buildings are totally destroyed and there are some fatalities. (See Table 1).

Building management system targeted attack scenario

BMS integrate several building management functions into one centralised system to increase efficiency and capability by permitting remote access and monitoring. Typical functions controlled by a BMS include CCTV and access controls, fire suppression, HVAC, power and lighting, lifts and energy, alarms and critical systems monitoring.

In this scenario, a group of sophisticated cyber terrorists identify vulnerabilities in HVAC systems in many buildings. Air conditioning units in server rooms and boiler systems become the primary target.

The attack involves shutting off air conditioning in server rooms resulting in servers overheating and catching fire. In coordinated attacks, boiler systems are tampered with causing explosions resulting in property damage and loss of life.

The damage to the servers cause a shutdown of operations in the building and nationwide disruption of business reliant on the computer networks. The servers and networks require rebuilding from scratch.

The boiler explosion undermines the structural integrity of the building forcing the occupants to relocate.The loss of life means the building is subject to an intense investigation by law enforcement. The explosion impacts property and buildings within several blocks of the explosion. (See Table 2).

The OECD and Cambridge reports will be made available via the ARPC website at arpc.gov.au from 18 March.

DrChristopher Wallace is CEO of Australian Reinsurance Pool Corporation.