Actuaries Institute

# Cyber Risk and the Role of Insurance

GREEN PAPER
SEPTEMBER 2022

## About the Actuaries Institute

The Actuaries Institute ('the Institute') is the sole professional body for Actuaries in Australia. The Institute provides expert commentary on public policy issues where there is uncertainty of future financial outcomes. Actuaries have a reputation for a high level of technical financial expertise and integrity. They apply their data analytic and risk management expertise to allocate capital efficiently, identify and mitigate emerging risks and help maintain system integrity across multiple segments of the financial and other sectors. Our public policy principles can be viewed at: https://actuaries.asn.au/public-policy-and-media/public-policy/policy-principles.

## About the profession

Actuaries use data for good by harnessing the evidence to navigate into the future and make a positive impact. They think deeply about the issue at hand, whether it's advising on commercial strategy, influencing policy, or designing new products. Actuaries are adept at balancing interests of stakeholders, clients, and communities. They are called upon to give insight on complex problems, they will look at the full picture. Actuaries analyse the data and model scenarios to form robust and outcome-centred advice.

This paper was commissioned by the Actuaries Institute and authored by Win-Li Toh and Ross Simmonds (both of Taylor Fry) and Michael Neary (DXC Technology).

While this Green Paper remains their own work, the authors would like to thank Thomas McCosker (Head of IT and Information Security at Taylor Fry) and Neil Curtis (Senior Executive Cybersecurity at DXC) for their contributions to the paper.



The Actuaries Institute acknowledges the traditional custodians of the lands and waters where we live and work, travel and trade. We pay our respect to the members of those communities, Elders past and present, and recognise and celebrate their continuing custodianship and culture.

# Contents

# Executive summary

Australians are more dependent than ever on technology. With the pandemic propelling trends that existed pre-COVID-19, technology, and therefore cyber risk, is now woven into almost every aspect of our lives and social fabric. In such an environment, it is crucial there is a vibrant and resilient risk management framework and infrastructure for cyber risk. Cyber risk insurance is a key part of that and the focus of this Green Paper.

## Cyber crime on the rise

In Australia[1], a cyber crime was reported every eight minutes over the past financial year – an increase of 13% on the previous year. Reported total economic losses in the year amounted to $33 billion, impacting government and the private sector, all sizes of organisations – from SMEs to the largest corporates – across industries and disrupting supply chains. Globally, 623 million ransomware attacks were recorded in 2021. That is 20 attacks every second and more than triple the number recorded in 2019.[2]

**Globally, 20 ransomware attacks occur every second – more than triple the number recorded in 2019.**

## Omnipresent and unpredictable risk

Cyber risk is a classic 'wicked problem' (Rittel and Weber, 1973). It is omnipresent, unpredictably dynamic and its root causes are entangled with other problems. For example, there are many motivators for cyber attacks, and the economics or expected payoff for cyber attackers is constantly improving. Further, Act of War exclusions typically found in traditional covers are difficult to apply in a cyber realm, where there are greater nuances as to where an attack may be attributed. It can be a combination of state actors or financial motives, and mere indications of fault are not enough to attribute fault 'beyond reasonable doubt'.

For cyber risk insurers and consumers, such characteristics challenge the usual conventions about whether a policy is fair and of value. How accurately does past claims experience inform future experience? Are previous terms and conditions for coverage appropriate? The issues may be complex, yet it is clear that protection is vital for economic resilience given the reported total economic losses of $33 billion last year.

No wonder cyber risk is consistently among the top risks identified by Directors, C-Suite executives, policymakers and regulators.

## Growth, capacity and sustainability

The cyber insurance market is small globally and even smaller locally. Cyber represents 4% of the Lloyd's market, less than 1% of the United States market, and only 0.4% of the local general insurance market. On the one hand, this

1 Australian Cyber Security Centre (2021b).

2 SonicWall (2022a).

suggests strong growth potential, some of which may come from reducing the extent of underinsurance, including through greater awareness of cyber insurance and its potential value.

Equally, however, if underinsurance is significantly addressed, there are questions whether the Australian market will have capacity because it would make cyber risk the largest, or one of the largest, lines of business. Is this sustainable given the 'wickedness' of the risk?

Scenario analysis is one tool that could assist business to understand the potential costs of poor cyber resilience, including reputational damage and time needed to rebuild trust. Actuarial projections give a clear picture of the impacts and value of cyber insurance and other mitigations on financial position and profitability over the longer term. Actuaries are well placed to provide organisations with insights to make evidence-based decisions about their cyber protections.

This Green Paper offers several solutions-focused discussion points, as we examine the complementary roles of government, business and insurers in creating a robust best-practice framework, where cyber insurance can thrive and offer better protection against cyber risk.

## Key points

- **Good cyber hygiene and security – not insurance – are the first line of defence.** These come from best-practice technology, specialist staff and widespread training. However, despite an increasing cyber spend by government and business, government entities are a long way off baseline standards of cyber security, while many businesses are also behind in their resilience against rapidly shifting risks.

- **A vibrant cyber insurance market will do more than provide financial recompense for risks that break through the first line of defence. It can also strengthen that first line, by offering clear signals and incentives to business – in the form of eligibility, pricing and sharing of insights – on best-practice standards.** Historically, this approach is in insurers' DNA. In traditional classes, insurers already have a track record in setting best-practice standards – think plimsoll line in marine insurance, or smoke detectors/sprinkler systems in commercial property insurance.

Importantly, **there are gaps in achieving this best-practice ideal,** notably:

- **A severe shortage of qualified cyber security personnel.** The global workforce needs to grow by 65% (from 4.2 million to 7 million cyber security professionals)[3] to effectively defend organisations' critical assets, with 8 in 10 breaches attributed to a skills gap[4].

  In Australia, Austcyber estimates around 7,000 more cyber security professionals are needed across all industries by 2024 to counter the growing threat. More recent research commissioned by cyber security firm CyberCX[5] more than doubles this and puts the shortfall at 30,000 over the next four years. This would require a five-fold increase in the number (currently estimated at 1,300[6]) of students in cyber security courses, although several organisations are undertaking their own training to meet the demand and offer an alternative pathway into the cyber security industry.

**A vibrant cyber insurance market can strengthen cyber hygiene and security by offering clear signals and incentives.**

3 (ISC)² (n.d.).
4 Fortinet (2022).
5 CyberCX (2022).
6 Bourlioufas (2022).

- **Limited understanding of the role of cyber insurance among Boards**, particularly a myth that control would be relinquished by taking out cyber insurance, with the insurer becoming a 'shadow director' in a cyber event. Improved education for Boards is vital to dismantle these misconceptions.

- **Limited education on cyber risks among SMEs**. Attacks are increasingly shifting towards smaller firms, which are exposed as easier targets, and where there is a lesser risk of repercussions. Yet only 20% of SMEs currently have cyber insurance, compared with 35% to 70% for larger organisations.

- **Achieving sufficient capacity and profitability in the market.** The tumultuous claims experience on cyber insurance over the past two years has reduced insurer appetite for this class, with reductions in policy limits and price increases to offset losses.

- **The challenges for insurers in managing accumulation risks,** of which Acts of War form a significant aspect, are beyond the bounds of risk the market has traditionally had to manage. With no geographical barrier to where claims can arise, the management of accumulation risks presents a key impediment to establishing a resilient and sustainable market for cyber cover. These risks are potentially large scale and catastrophic, and are limiting the amount of cover insurers can offer.

- **Cyber hesitancy in seeking the right insurance solutions,** with some organisations choosing not to take out cyber insurance in the belief that having the insurance would make their company a bigger cyber target. Ultimately, any business that utilises technology or has access to sensitive or valuable data will be at risk of being a target, whether or not they have insurance protection.

Collaboration between all stakeholders is critical in plugging these gaps, as the issues are too vast to be solved in isolation. For example, effective regulation will take into account the shortage of cyber security professionals that may impede compliance, and be combined with investment towards filling this need. Collectively, we have the ability to make meaningful decisions that will create a resilient and effective insurance market, and uplift the cyber security of the nation as a whole.

## Tips for navigating this paper

For readers already well read in cyber risk and looking for further information, we recommend moving to Section 4 – Understanding cyber insurance and its role in mitigating risk, and Section 5 – Conclusions, about the impediments to achieving a best-practice framework and how to plug these gaps.

For other readers, contextual information is available in Section 2 - Evolution of cyber risks and the impact on businesses, and Section 3 - How government and businesses are responding to increasing cyber risk.

Readers will not find material on the following topics, as there is already considerable publicly available information:

- The hazard of whether or not to cover ransomware;
- Handbook for board directors;
- Attacks perpetrated on individuals (we consider entities only); and
- Underwriting/pricing guide for insurers.

**Despite an increasing cyber spend by government and business, government entities are a long way off baseline standards of cyber security.**

# Evolution of cyber risks and the impact on businesses

2

## Section overview

- Cyber risk is growing at unprecedented levels, with the increasing use of technology and as computers become increasingly networked. Globally ransomware attacks have more than tripled in two years.
- The accessibility of Ransomware as a Service (malware products), combined with the development of crypto currencies enabling untraceable payments, has super-charged the growth of cyber attacks. This has brought more organisations of different types and sizes under the widening net of cyber criminals. No organisation is immune.

## 2.1 What is cyber risk?

Cyber security risk is the probability of exposure or loss arising from a cyber attack or data breach on an organisation[7], which may result in financial harm, disruption or reputational damage.

For the purposes of this paper, we consider the characteristics of cyber risk, focusing on the impacts on **business and government.**

### Defining features

The global nature of technology means businesses can be **attacked from any location in the world**. This creates a much larger exposure to potential criminal activities than more traditional localised crimes.

In addition, in many other contexts damage needs to have materialised to result in a cost to a business. In the case of cyber, **a cost may be incurred without the damage materialising.** This includes extortion to prevent an occurrence. In this category is ransomware.

The cyber risks themselves may originate from both **internal and external actors**, poorly configured systems or system vulnerabilities.

The global nature of technology means businesses can be attacked from any location in the world.

### Types of loss – Tangible and intangible

Overall, cyber risk arises from the use of any information technology, be this networks, applications or hardware. When this risk materialises, it may result in a loss, and these losses may impact several tangible or intangible areas, such as:

- **Financial** – Losses arising from remediation of the damage, from the direct loss of business due to interruption, fraud losses from payments

7 Tunggal (2022).

to other parties, and losses arising from the payment of ransoms to actors or regulatory fines.

- **Reputational** – Loss of customers and business from a loss of trust and/or reliability. Unlike some other forms of business interruption, cyber may result in ongoing brand damage.
- **Operational** – Loss of data, or loss of hardware or software use, leading to operational impairment, a loss of production and/or supply.
- **Intellectual property/Intelligence gathering** – Loss of intellectual property such as designs or research, and loss of commercially sensitive information such as tender responses.

## 2.2 How has cyber risk evolved?

Cyber risk had its origins at the start of computing and networking technologies. While the nature of the risk has changed along with the technology, the reasons for the risk arising remain largely the same **– direct or indirect financial gain.**


### French connection

As early as 1834, the French telephone system was breached for financial gain[8]. Over time, various attacks have occurred accessing databases and systems either to obtain data or for gratification. Another early example includes in 1976 a 13-year-old using a combination of social engineering and dumpster diving to circumvent the punch-card system being used by the Los Angeles bus system[9].

### Advent of computers

As computers became increasingly networked, the opportunity to access them also increased and the risk of attacks increased. Similarly, the use of common software and hardware creates opportunities for large-scale attacks. The sudden change in work practices over the past two and a half years, with remote working during the pandemic, has further exacerbated the issue. In addition, the limits to software liability, unlike other products, generally puts the onus and costs of attacks on the user.

### Why cyber attacks happen today

Many cyber attacks occur opportunistically to exploit weaknesses in IT systems. In these instances, it is difficult to attribute the motivation, which could be a combination of espionage, subversion, sabotage and financial gain.

Cyber security expert and former Amazon and Microsoft adviser Tim Rains explores the motivation for self-gain in his book *Cybersecurity Threats, Malware Trends, and Strategies*[10]. He believes it falls into six key areas.

1. **Notoriety** – The attacker wants to prove they are smarter than the technology companies and their victims.
2. **Profit** – Generate profit directly through fraud or indirectly through the value of data (see next point) or extort payments e.g. via ransomware.
3. **Economic espionage** – Obtaining intellectual property to gain a competitive and economic advantage.
4. **Military espionage** – Governments want to understand the military capabilities of their adversaries, including conducting counter-intelligence.

**Many attacks occur opportunistically to exploit weaknesses in IT systems, making it difficult to attribute motivation.**

8 Standage and Stevenson (2018).
9 Agarwal (2016).
10 Rains (2020).

5. **Hacktivism** – Attacks against organisations and institutions based on disagreements on political or philosophical issues, which at its extreme can be deemed terrorism.
6. **Influencing elections** – Using cultural manipulation and information warfare to help nations achieve foreign policy objectives.

Revenge could also sit in several of the above motivations.

## How malicious actors thrive

### *Human error and the importance of awareness*

Even with the best technological defences, most cyber events are due to human error, such as phishing attacks, as opposed to software deficiencies. A recent IBM study[11] assessed that 95% of cyber security breaches are primarily caused by human error, highlighting the importance of education and awareness alongside the technological developments.

### *Ability to adapt and exploit at pace*

For the risks driven by criminal activity, the types of attacks can rapidly evolve as cyber criminals continually search for the easiest method that can extract the highest payout. An example of this evolution is the significant increase in the frequency of ransomware attacks over the past few years.

### *Exposing the weakest link with the most promise*

Globally, 623 million ransomware attacks were recorded in 2021 – that is 20 attacks every second and more than triple the number recorded in 2019.[12] The increase in these types of attacks have risen sharply as cyber criminals have realised that disrupting a company's IT services using ransomware may be as profitable as stealing information and selling it. The development of crypto currencies has also made it easier for cyber criminals to receive payments outside the usual banking and payments controls.

Figure 1 illustrates this realisation and altered approach, showing changes in ransomware attack vectors over time. Importantly, phishing now accounts for just as many attacks as Remote Desktop Protocol (RDP) compromise (that is, allowing remote access to a system over a network connection due to weak passwords or unrestricted port access).

**95% of cyber security breaches are primarily caused by human error.**

**11** World Economic Forum (2022).

**12** SonicWall (2022a).

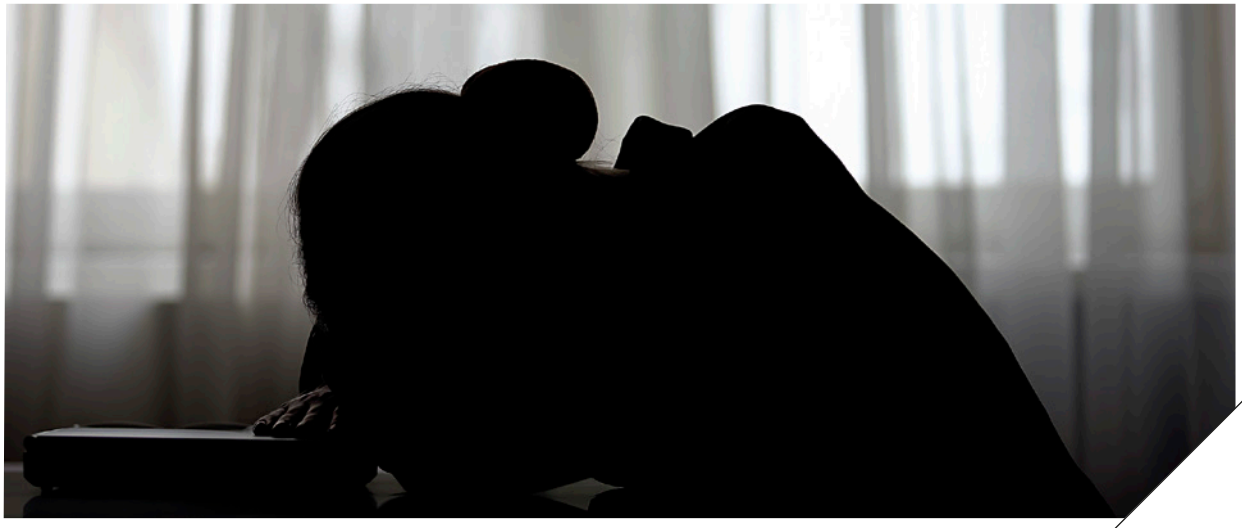
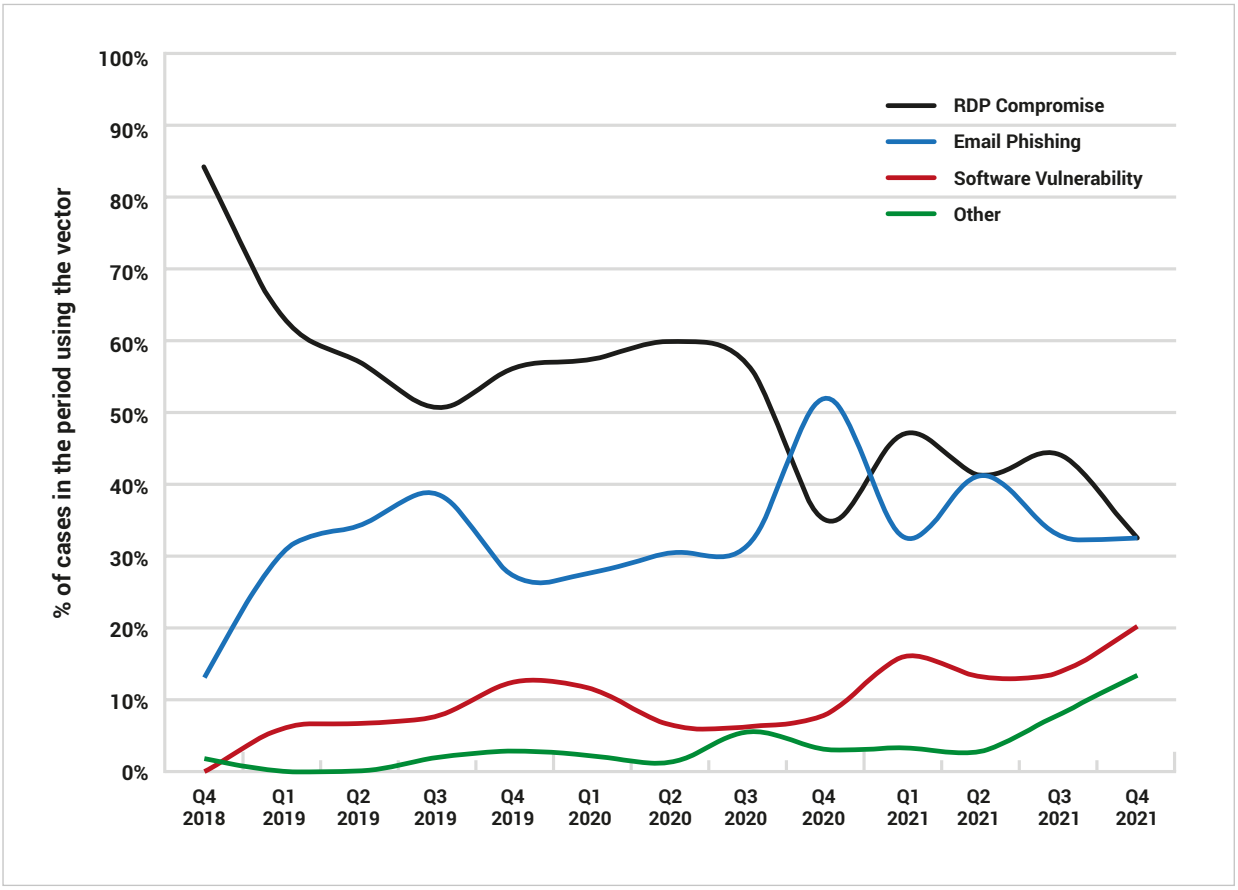


**Figure 1 – Change in ransomware attack vectors over time**




*Source: Coverware (2022)*

## Cyber crime as a business model – "It's like eBay"!

The accessibility of cyber crime services, such as Ransomware as a Service (RaaS), have increasingly opened the market to a growing number of malicious actors without significant technical expertise and without significant financial investment.

### *Dark partnership*

An example of this is a revenue-sharing scheme devised by a RaaS group in conjunction with hackers. Any hacker who successfully carries out an attack passes a percentage of the bounty to the malware developers. The arrangement permits the developers to continue focusing on malware development, leaving the task of seeking out new attack targets to others. It also allows the developers to hide behind a curtain.

"It is a marketplace that involves services, products and goods," Mark Arena, CEO of the cyber crime intelligence firm Intel471, told CBS News. "It's like eBay."

**Hot topic for decision makers** – Current RaaS models have made cyber crime more accessible to malicious actors, without the need for big investment or technical expertise. This has super-charged the growth in cyber attacks and the risk for all businesses.

## Snapshot – The mathematics of ransomware

Here we look at the business model from the adversary's perspective.

### *Business motivated by profit*

It may be useful to think of Ransomware as a business – motivated by profit. As with any profit-driven business, the aim is to maximise profits – i.e. maximum revenue at lowest cost. As a target, the questions are then: 'Is my business attractive?' and 'What can I do to make my business unattractive to cyber criminals?'

Academia has been creating models on just this topic. Hack and Wu in their 2021 paper[13] outline an equation to evaluate the return from a successful ransomware compromise.

$$P = \sum_{i=1}^{N} (r_i * m_i * l_i) * f(i) - c_i$$

Where:

- **P** is the total profit taken by the criminal from **N** number of victims.
- $\mathbf{r_i}$ is the final ransomware demand on case **i**.
- $\mathbf{m_i}$ is the percentage left after paying the commission fee for the RaaS platform, which could cost anything from 10%-30% of the ransom, or 0% for adversaries using in-house ransomware tool kits.
- $\mathbf{l_i}$ is the percentage left after exchanging the cryptocurrency to 'clean' currencies.
- **f**(i) is the final decision made by the victim to pay or not, and can either be 0 (not pay) or 1 (pay). It can also be between 0 to 1, if the victim pays, but some of it is recovered (as in the Colonial Pipeline case).
- $\mathbf{c_i}$ is the cost of carrying out the attack, as explained below.

### *The cyber crime equation in action*

Using this formula, we can calculate the adversary's profit for N number of victims.

Let us assume we have two victims, the ransom demand ($r_i$) is $100,000 in Bitcoin in both cases, the RaaS fee is 20% ($m_i$ = 80%) of the ransom, the exchange cost is 10% ($l_i$ = 90%), only the second victim pays (f(i) = 0 in the first case and 1 in the second case), and the cost of carrying out the attack is $50 ($c_i$).

In the first case, the profit is ($100,000 * 0.8 * 0.9) * 0 – $50 = -$50 (i.e. a loss). In the second case, the profit is ($100,000 * 0.8 * 0.9) * 1 – $50 = $71,950. The total profit of the two ransom attacks is therefore $71,950 + (-$50) = $71,900.

The mathematics can be used to assess the return from different strategies. For example:

- An organised cyber crime group that hunts only for big targets and asks for millions of dollars but only 5% of the victims paid, versus
- Another group that hunts small and medium size targets and only asks for a few thousand dollars but 20% of the victims paid.

Evidently, these two business strategies lead to different profit gains, and the mathematics can help to determine the chosen path. Furthermore, the cost for operating a criminal operation and achieving the initial compromises should be included in the calculation.

### *Insight through a criminal lens*

The model provides an interesting perspective from 'the other side'. It also raises the question of how insurers' models mirror those of the attacker. **The authors strongly recommend not letting attackers know if you have cyber insurance and not to save any insurance documentation on accessible servers**, as this information has been used against organisations when negotiating a payment. This is akin to kidnap and ransom insurance where policyholders are advised not to publicise their policy or which executives are covered, which could void the policy if so, due to the increased risk of being kidnapped which undermines the principles of insurability[14].

**13** Hack and Wu (2021).

**14** Principles of insurance – Utmost good faith, Insurable interest, Indemnity, Contribution, Subrogation, Loss minimisation and Proximate cause.

In the next section, with the cost base of attacks ($c_i$) reducing due to the accessibility to ransomware tools, and as larger firms increasingly decline to pay ransoms (f(i)), we see evidence of the model in action as smaller firms are increasingly exposed.

## 2.3 What are the impacts for businesses?

### No organisations are immune, as the cyber criminals' net widens

The evolving nature of cyber attacks also means that as the type of attacks change, the underlying nature of the businesses that are targeted are also changing – with more companies coming under the widening ambit of cyber criminals.

Prior to the increase in ransomware attacks, criminal cyber attacks were focused on illegally accessing data that could then be monetarised. The targets for these types of cyber attacks were data rich organisations in the retail, health and financial services industries.

Ransomware attacks focused on disrupting IT services will instead focus on industries that will be unable to operate as a result, such as the manufacturing, food and energy industries. As these organisations had not been targets before, they have likely not invested as much in their information security and are more vulnerable to the widening focus of cyber criminals.

**Ransomware attacks ... will increasingly target industries unable to operate as a result, such as manufacturing, food and energy. No organisations are immune, from SMEs to global corporates.**

#### *Increasing losses across all sectors*

In Australia[15], over the past financial year, a cyber crime was reported every eight minutes, an increase of 13% over the previous year. Reported economic losses in the year amounted to $33 billion, impacting both government and the private sector, all sizes of organisations from SMEs to the largest corporates, across industries and disrupting supply chains.

#### *SMEs' vulnerabilities exposed*

No organisations are immune, from SMEs to the largest global corporates. In 2021, 75% of ransomware attacks were directed at companies with fewer than 1,000 people.

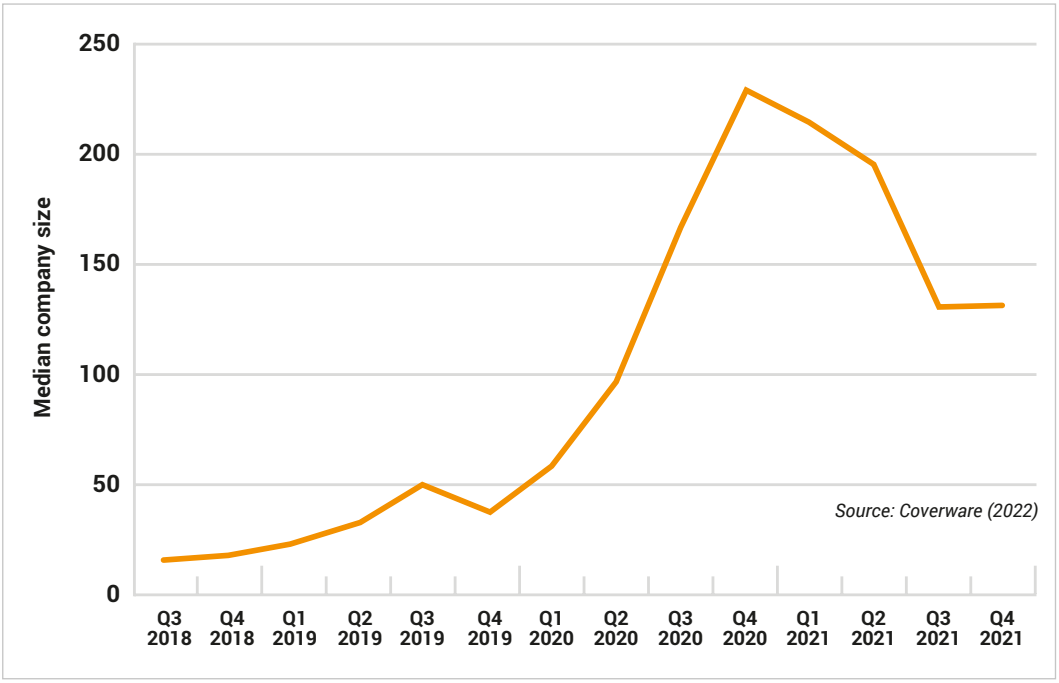
Recent evidence points to a shift in attacks towards mid-sized firms (see Figure 2), which are exposed as easier targets, and where there is a reduced risk of repercussions.

Notably, larger companies tend to have more robust systems with less vulnerability to opportunistic attacks. In addition, attacks on these organisations tend to have a higher profile and represent a greater risk of government intervention. An example of this was the Colonial Pipeline attack in May 2021 that drew FBI involvement, with the responsible party ultimately identified and most of the ransom recovered.

**Hot topic for decision makers** – Recent evidence shows a shift in attacks towards smaller firms, which are exposed as easier targets. No organisations are immune.

15 Australian Cyber Security Centre (2021b).

**Figure 2 – Median size of companies (by number of people) falling victim to ransomware**




## Key threats and trends over 2021

The risk to business is high. The Australian Cyber Security Centre (ACSC), which leads the Australian Government's efforts to improve cyber security, identified the following key cyber security threats and trends in the 2020–21 financial year.

- **Exploitation of the pandemic environment** – COVID-related spear phishing emails targeted individuals, while ransomware targeted health services especially, attempting to access intellectual property and sensitive information about Australia's response to COVID.
- **Disruption of essential services and critical infrastructure** – About one-quarter of incidents related to critical infrastructure or essential services (e.g. health, food distribution, energy sector) underscoring vulnerability, lost revenue and the potential for harm or loss of life.
- **Ransomware** – This poses one of the most significant threats to Australian organisations, with a 15% increase in the 2020–21 financial year. Criminals were aided by growing sophistication in dark web tools and extortion tradecraft, disrupting professional, scientific and technical organisations, as well as those in healthcare and social assistance.
- **Rapid exploitation of security vulnerabilities** – Criminals operated at speed and scale, sometimes within hours of public disclosure, patch release or technical write up, especially if the proof of concept code identifying system vulnerabilities was also released.
- **Supply chains** – The threat to supply chains is high, particularly where well-resourced criminals compromise widely used software products and services to gain access to a vendor's customers.

## The potential for significant disruption due to cyber attacks across industries is very high.

- **Business email compromise (BEC)** – The average loss per event has increased to more than $50,600, at least one-and-a-half times higher than last financial year. Cyber criminals continue to exploit the increase in remote working across business and government with enhanced and more organised methods.

Looking further afield, Lloyd's of London also acknowledges the high level of threat, warning that a major cyber attack could cost as much as $163 billion (£92 billion) to remedy. The UK Government reported that 46% of businesses have had a cyber attack or breach in the past 12 months. These statistics may raise concern among businesses that the growing risk is not necessarily being matched by the security procedures being put in place.

**Hot topic for decision makers** – As cyber criminals increasingly find different, more impactful and sophisticated ways of accessing systems and targeting different types of companies, the potential for significant disruption across industry is very high.

In the following sections, we look at how businesses, government and insurers are approaching this increasing risk, and the role of cyber insurance within a robust risk mitigation framework.

# How government and businesses are responding to increasing cyber risk

3

## Section overview

- Cyber is a big priority for government and business, with both increasing their cyber spend.
- Despite significant investment and initiatives, cyber losses continue to increase as risks evolve and become more sophisticated.
- A skills gap and severe shortage of qualified cyber security personnel are the major factors in cyber security management.
- Adoption of information security frameworks are optional for businesses, which means there is no united approach to mitigate threat across organisations.

**In the March 2022 Budget, the Government announced its biggest ever investment in Australia's cyber preparedness.**

## 3.1 What are governments doing?

With increasing connectivity and exposure to cyber-criminal activity, governments around the world are taking an active role in cyber security. This role is across several channels, including investment in cyber preparedness, regulation, facilitating industry developments and information exchange, research, collation of data and general guidance.

Current developments in Australia encompass **financial investment, new legislation, regulatory reform consultation and various initiatives**.

### Investment in cyber preparedness

In the latest **federal budget**, delivered on 29 March 2022, the Australian Government announced its "biggest ever investment in Australia's cyber preparedness"[16], of $9.9 billion spread over 10 years. This is expected to enable Australia's electronic spy agency, the Australian Signals Directorate (ASD), to double in size and triple its offensive cyber capabilities.

This announcement follows the **Government's Cyber Security Strategy 2020** established in August 2020[17], a $1.7 billion 10-year plan to achieve a vision of 'a more secure online world for Australians, their businesses and essential services'. The strategy recognises that this vision will be delivered through the collective actions of government, businesses and the community.

### Legislation and proposed regulatory reform

#### *New Acts*

As part of the Cyber Security Strategy 2020, the Government introduced the Security Legislation Amendment (Critical Infrastructure) Act 2021[18], in

16 Commonwealth of Australia (2022).
17 Commonwealth of Australia (2020).
18 Department of Home Affairs (n.d.a).

**Reforms are likely to expand what counts as personal information and increase the penalties for serious breaches to about 10% of the organisation's annual domestic turnover.**

December 2021, expanding the coverage of entities and sectors that are considered critical infrastructure entities. This was followed by the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 in April 2022.

These Acts introduced **new obligations** for critical infrastructure entities, with the purpose of protecting critical infrastructure and essential services.

Reforms are also underway on the Privacy Act, which look to expand what counts as personal information and **increasing the penalties** for repeated or serious breaches of privacy from about $2 million to the greater of $10 million, three times the benefit obtained from any misuse of information or 10% of the organisation's annual domestic turnover.

### *Inviting consultation*

The Government opened consultation in July 2021 on options for regulatory reforms and voluntary incentives to strengthen cyber security of Australia's digital economy[19]. The aim was to set clear expectations for businesses to manage cyber risks, providing increased disclosures and transparency about the security of technology products, and improving consumers rights.

After speaking with more than 770 businesses, community groups and individuals, the Government received 143 written submissions. At this stage, no dates have been announced as to when any of these proposed policies may be implemented.

## Initiatives

### *Ransomware responses*

The Government announced its Ransomware Action Plan (RAP) in October 2021, which aims to build Australia's resilience, strengthen responses and strengthen the criminal law regime. It notes that the Government does not condone paying ransomwares.

The RAP also notes that legislative reforms will be developed to **mandate ransomware incident reporting** to the Australian Government.

Internationally, there have been calls to ban ransomware payments, most notably in the United States[20]. However no international jurisdiction has yet made the payment of ransomware illegal.

### *Guidance and education*

The Australian Cyber Security Centre (ACSC) forms part of the Australian Signals Directorate (ASD), providing a Learn Hub with resources such as interactive tools and guidance catering for different groups, from individuals to SMEs, critical infrastructure and government.

Additional educational initiatives include ACSC **news and alerts on credible cyber threats** to Australian organisations and various government **grants for cyber training** for 40 to 100 students annually[21]. Another initiative includes **ACSC's eight essential mitigation strategies**, known as the Essential Eight, providing a recommended baseline for organisations to protect against cyber threats. Implementation of the Essential Eight forms part of the mandatory requirements under the Protective Security Policy Framework. The framework

**19** Department of Home Affairs (n.d.b).

**20** Glover (2022).

**21** Leibel (n.d.).

defines the Australian Government's security classifications and associated handling protections of official information.

Audits have continually shown **most public sector agencies[22] are well below these Essential Eight minimum standards**. An ANAO audit[23] in 2021 revealed only one in 18 of the largest departments and agencies were fully implementing the controls, with most found to be 'significantly below' current requirements. With effect from June 2022, all entities that are **mandated to comply** with the Essential Eight will undergo comprehensive audits every five years.

### *Discussion points for decision makers*

#### *Investment, legislation and regulatory reform proposals*

- For government actions to be transparent, progress and impact need to be monitored. Currently, there is no monitoring tool for achievement in government cyber spend. **Could a frequent monitoring tool help drive intended outcomes and accountability?**
- While the benefits of protecting critical infrastructure are clear, new legislation places additional obligations and costs on essential services businesses. **How can industry and government work together to spread the benefits across business and government?**
- With any new policies requiring time for careful consultation and regulatory approval, there is a real risk of becoming redundant before they are implemented. **As cyber attacks continue to gain in creativity and sophistication, what systemic changes could improve responsiveness?**

#### *Initiatives for guidance and education*

- Government entities are a long way off baseline standards of cyber security. **What is the value of introducing incentives to comply?**
- With government putting pressure on industry, given the $9.9 billion committed to building public sector capability, **how can the general population, critical infrastructure or business education be more comprehensively catered for other than via grants?**

## APRA and the question of compliance

Financial institutions that are regulated by the Australian Prudential Regulation Authority (APRA) are required to comply with *Prudential Standard CPS 234 Information Security* (CPS 234). This standard was introduced in 2019 and requires APRA-regulated entities to comply with a range of information security protocols across the organisation, from Boards to individuals. These include clearly defined responsibilities, appropriate capabilities as well as controls to protect information assets, and notifying APRA of any incidents.

### *Testing times*

In 2021, APRA undertook an independent assessment of a pilot set of entities' compliance with CPS 234, which has led to APRA stating that **boards need to take a more active role** in:

**Audits have continually shown most public sector entities are well below minimum standards.**

**22** Non-corporate Commonwealth entities, of which there are 98 currently.

**23** Sadler (2021).

- Reviewing and challenging information reported by management on cyber resilience;
- Ensuring their entities can recover from high-impact cyber attacks; and
- Ensuring information security controls are effective across the supply chain.

This review highlights the need for all organisations to proactively manage their own cyber resilience as well as across their supply chain. While CPS 234 applies only to APRA-regulated entities, the requirements outlined by CPS 234 are consistent with the steps that all organisations should be taking to maintain a high level of cyber hygiene.

**Identifying the gaps** – There is a gap where Boards of regulated financial institutions need to gain a deeper understanding and take a more active role in cyber governance. This is also relevant for non-financial institutions.

### *How increased APRA data could be good for business*

One of the current limitations for insurers writing cyber insurance is a lack of available data. In March 2021, following a consultation with the insurance industry, APRA expanded its data collection to include cyber insurance and management liability as a separate class of business in the National Claims and Policies Database. This change applies for the 31 December 2021 half year. The new reporting class will only apply to standalone cyber insurance policies.

While the data reported on by APRA will be accumulated, it will provide some basic industry statistics on cyber insurance risks written in Australia and is a **good start towards assisting insurers in setting cyber insurance premiums.**

## Further engagement with insurers

The Government's 2020 Cyber Strategy was launched in response to the recommendations of a cyber security strategy industry panel. One of the recommendations of the panel (number 30 of 60) was to *"work with the cyber insurance industry to improve access to reliable actuarial data and develop best practice approaches to nudging the cyber security hygiene of policy holders"*. While the panel is independent – and so the Government is not committed to following its recommendations – it is worth noting that the cyber security strategy released by the Government does not explicitly mention the insurance industry.

**It is worth noting that the cyber security strategy released by the Government does not explicitly mention the insurance industry.**

### *A broader government focus*

The Government's focus appears to be on the wider picture, in setting a broad framework for enhancing its offensive cyber capabilities, protecting critical infrastructure and providing general guidance. Our understanding is that there is not a specific focus on solutions for insurance issues at present, with Government looking at other priorities as insurers grapple with providing cover for the increasing volume, sophistication and changing nature of cyber risks.

The 2021 triennial review[24] of the Australian Reinsurance Pool Corporation (ARPC) considered the extension to covering physical property damage arising from cyber terrorism, but this was rejected on grounds that cyber insurance is an evolving market and there is yet to be a clear and evident market failure from this cause. More recently, a paper for The Geneva Association acknowledged

**24** The Treasury (2021).

the need to "adapt to the changing threat landscape".[25]

In the foreword to that paper, the Managing Director of The Geneva Association, Mr Jad Ariss, and the President of the International Forum of Terrorism Risk (Re) Insurance Pools and CEO of the Australian Reinsurance Pool Corporation, Mr Christopher Wallace, state:

> *"It is clear … that the development of a sustainable private cyber re/insurance market to cover the full scope of cyber risks will ultimately be contingent on the development of some form of public-private partnership (PPP) or government backstop. PPP blueprints are already in place in several countries to share exposures to natural catastrophe as well as terrorism risks and nuclear risks. Cyber risk comes with its own set of complexities, yet the constraints on the private re/insurance sector's capacity to absorb losses from an extreme cyber incident are becoming increasingly obvious."* [26]

**Identifying the gaps** – The gap in current policy for investing in insurance or working with the insurance industry presents opportunities for the Government to engage with insurers to expedite a vibrant cyber market and greater protection for businesses.

## Severe skills shortage – A cross-sector challenge

Austcyber[27] together with the cyber security industry, has identified a skills gap and shortage of qualified cyber security personnel as the major factor in cyber security management today. **Their sector competitiveness plan (2019) indicates that nearly 17,000 more cyber security professionals are needed by 2026 to effectively protect critical assets in Australia.** A more recent estimate is for around 7,000 more professionals needed across all industries by 2024. More recent research commissioned by cyber security firm CyberCX[28] more than doubles this and puts the shortfall at 30,000 over the next four years. **This would require a five-fold increase in the number (currently estimated at 1,300[29]) of students in cyber security courses**, although several organisations are undertaking their own training to meet demand and offer an alternative pathway into the cyber security industry.

There are many factors impacting the ability to ensure the right skillsets are being developed and the appropriate investment in cyber security education is made. These include:

- Lack of coordinated focus in research and commercialisation;
- Scattered public funding weakening Australia's ability to lead on innovation;
- Market barriers holding back ecosystem development; and
- Lack of robust measurement limiting commercial decision making and ability to track progress.

This shortage in Australia is mirrored globally, where the workforce needs to grow by 65% (from 4.2 million to 7 million cyber security professionals)[30] to effectively defend organisations' critical assets.

**A skills gap and severe shortage of cyber security professionals represents a major cross-sector challenge to effectively protect critical assets in Australia.**

25 Carter, Pain and Enoizi, 2022.

26 Carter, Pain and Enoizi, 2022, p.5.

27 Austcyber is the Australian Cyber Security Growth Network, with the aim of building a network of skilled cyber professionals. Further information is available at https://www.austcyber.com/

28 CyberCX, 2022

29 Bourlioufas, 2022.

30 (ISC)² (n.d.).

**Discussion point for decision makers –** Training and general education needs are high, with a time lag in building capability of people and capacity. How can tertiary educators, government and companies who undertake their own training collaborate to ensure the right cyber/IT skillsets are being developed and appropriate investment in cybersecurity is being made, given the urgent need for qualified personnel?

## 3.2 What are businesses doing?

### Cyber risks are top of mind for large businesses in 2022

**More than 75% of risk professionals have increased their cyber budgets and intend to continue to increase their spend**, according to Airmic 2021[31], a survey of risk and insurance professionals. Stepping up employees' training and education are other areas organisations are looking to improve. The survey also found front-of-mind risk for these professionals is **business interruption following a cyber event**, with businesses turning increasingly to insurance for additional protections. But increasing underlying risk is making it harder to get cover as insurers look to limit their exposures and increase premiums.

In another study, the *2022 Directors' Liability Survey Report*[32], **cyber attack, data loss and cyber extortion** are ranked as the top three risks for directors, above regulatory risk, health & safety/environmental risks and climate change. Of respondents to the survey, 73% globally and 61% in Australasia, deemed cyber attacks to be a 'very significant' or 'extremely significant' risk to their business – with the lower figures in Australasia possibly explained by the relatively less mature regulatory environment and less frequent targeting of companies.

**In one study, cyber risks rank above regulatory risk, health & safety risks and climate change for directors.**

### Cyber capability, assisted by technology

Cyber capability in detecting and responding to risks has been assisted by technology. While the techniques do not often change, there has been a major shift in the tools applied over time.

For example:

- In 2010, Antivirus software was most commonly used in devices such as laptops, desktops and servers. This software maintained a dictionary of threats, needed to be updated at least daily and recognised **only known threats.**
- In the early 2020s Endpoint Detection and Response (EDR) emerged to stop **threats that are not yet known**. It may use artificial intelligence (AI) and threat intelligence along with cloud computing resources.
- Further to EDR are Network Detection and Response (NDR) platforms, which detect anomalous network traffic and block malicious traffic before it infects or compromises other hosts. The leader in this market segment is DarkTrace, which uses **autonomous cyber AI** to interrupt in-progress cyber attacks in seconds.

### Creating a cyber-aware culture

As the risks have evolved, cyber security frameworks have had to adapt to the changing complexity. Cyber-aware cultures are becoming a necessity for

**31** Airmic (2021). Airmic is a leading UK association for everyone who has a responsibility for risk management and insurance for their organisation.

**32** WTW and Clyde & Co. (2022).

businesses and increasingly expected in working with government and third-party suppliers. The proliferation of insurtechs and other service providers (such as Clyde & Co) attest to the focus businesses are investing in cyber solutions.

Cyber risks are increasingly being embedded within companies' enterprise risk management frameworks, which are then used to develop their information security management systems (ISMS), with some seeking out formal certifications.

### *Formal frameworks for information security*

Some of the widely recognised and recent ISMS certification take-ups are:

- **ISO 27001** – This is the best practice standard for managing information security within all types of organisations, especially in Australia[33].Take-up has more than doubled in two years, with 562 certifications in Australia in 2020, vs 325 and 264 in the two previous years[34].
- **COBIT (Control Objectives for Information and Related Technology)** – Similar to ISO 27001, but COBIT 2019 additionally aims to help an organisation map its own business goals to its IT goals. Unlike ISO 27001, ISACA does not offer an ability for organisations to be COBIT certified.
- **National Institute of Standards and Technology (NIST) Cybersecurity Framework** – In the US, NIST aims to have a uniform set of standards for organisations across industries and for them to keep updated through the US Cybersecurity & Infrastructure Security Agency (US-CERT).
- **Centre for Internet Security (CIS)** – The CIS is a non-profit that harnesses the power of a global IT community through its "best practice guidelines for computer security". These are technical measures to protect from cyber attack, rather than rules of compliance, governance and risk.
- **Essential Eight Maturity Model (Essential Eight)** – A mandated baseline standard series of technical recommendations for eight mitigation strategies. In NSW, government agencies must submit an annual maturity assessment[35]. Audits have continually shown most agencies are well below these minimum standards.

**Hot topic for decision makers** – In Australia, adoption of information security frameworks are optional for businesses, which means there is no united approach to mitigate threat across organisations. However, for any mandatory standards to be effective, clear guidance and assistance would be required from government beyond compliance, in a culture of strong collaboration between business and government.

## Supply chain security under attack

For many organisations, the risks from supplier relationships have also increased with the greater reliance on automation, such as B2B and Software as a Service (SaaS). This has potentially far-reaching consequences as demonstrated by the Kaseya ransomware incident in 2021. The Kaseya platform remotely monitors other IT providers for phone, email, firewalls and networks. More than 1,500 companies in the US were impacted down the supply chain as a consequence of malware implanted on Kaseya's platform.

The risks from supplier relationships have also increased with the greater reliance on automation.

33 International Organization for Standardization (2013).

34 isPartners (2022).

35 Sadler (2021).

Cyber losses continue to grow as the risk evolves and with the time lag in training enough skilled cybersecurity personnel.

Many (especially larger) organisations are formalising their vendor management policies beyond traditional payment term arrangements, requiring security screening to be completed, and using third-party cyber-risk platforms, such as CyberGRX, BitSight and UpGuard.

Organisations that adhere to any of the major cyber frameworks need a vendor management policy to address the 'security in supplier relationships' and related controls.

## How are SMEs responding to cyber risk?

With more than two million SMEs in Australia, an ACSC Small Business Survey Report in 2020 revealed that almost 50% of them spend less than $500 on cyber security on average, and almost 50% had poor cyber security practices.[36] With the majority of SMEs having fewer than 20 staff, the report highlighted the issue of having to manage competing priorities with fewer staff.

This, combined with evidence pointing to a shift in focus of cyber attackers towards smaller firms (see Section 2.2), is clearly problematic. Some small firms, such as conveyancers, that handle high volumes of personal information and monetary transfers, would be **attractive targets for cyber criminals.**

The ACSC has guidance material directed at SMEs on its site, and has also provided grants to educational institutions aimed at assisting SMEs (see Section 3.1). However, awareness of these materials is low among SMEs.

### Hot topics for decision makers

- SMEs are not engaging effectively with government education.
- Businesses are taking action, especially larger ones, but risks continue to increase at a faster rate (see Section 2). While plenty of tools exist, there is no driving or legislated requirement to take action. Audits indicate that the market is some years off and too immature to meet legislation.
- Not all IT providers' standards are equal. Not all Boards are equal. Even financial institutions with large IT spends are behind in managing cyber resilience.
- Support for SMEs is inconsistent, and awareness of guidance materials is low. With evidence pointing to a shift in focus of cyber attackers towards smaller firms (see Section 2.2), there will need to be a stronger, more targeted focus on SME needs.

Despite significant investment by government and business, cyber losses continue to grow as the risk evolves and with the time lag in training enough skilled cyber security personnel.

In the next section, we look at cyber insurance and its role in mitigating this risk. Can a vibrant cyber insurance market help to fast-track a solution to the problem? If so, what needs to be in place for this to happen?

**36** Australian Cyber Security Centre (2021a).

# Understanding cyber insurance and its role in mitigating risk

4

## Section overview

- Cyber insurance forms a key part of a robust risk management framework – the best insurance underwriting practices have the potential to actively help increase cyber protections and reduce the likelihood and impact of a cyber incident. However, market capacity is limited and the capability across insurers is still vast.
- An insurance approach to assessing risk would focus organisations on the bare minimum needed to obtain protections – the first year may be hard for them, but processes will be easier to maintain once implemented and will be an important step towards the maturity of cyber security across the nation.

## 4.1 Cyber insurance 101

As cyber risks evolve, so too cyber insurance products are having to rapidly evolve to meet these changing needs. We look at how cyber insurance has developed over time, the main issues for cyber insurance amid rapid change and its role within a robust risk management framework.

### Where it all began

Cyber insurance policies were first developed in the late 1990s for technology companies. These policies provided **third party cover** (the costs incurred by clients of the insured company due to some fault of the insured party).

In 2003, California enacted the *Security Breach and Information Act*. This law required companies to notify all affected residents if their personal information had been accessed by an unauthorised party due to a security breach. Most US states followed California and introduced similar Acts. This change led companies to seek **first party cover** for cyber risks in addition to third party cover. It also extended the market for cyber policies beyond technology companies.

### Evolving to keep pace

As the underlying risks and threats have gained in sophistication, the cover provided by cyber policies has had to evolve to keep pace. Additionally, increasing reliance on technology has broadened the range of businesses wanting to protect their risks with cyber insurance products – and these companies have differing needs. The focus for some are technology disruptions and business interruption cover. Other data-rich organisations may seek cover for data breaches, compensation to third parties and brand restoration.

The evolution of cyber insurance means there is no one standard cyber insurance policy. An Organisation for Economic Cooperation and Development (OECD)[37] paper encouraging clarity in cyber insurance coverages notes that current cyber insurance policies protect businesses against six main types of cyber incidents.

- **Data confidentiality breaches,** covering costs associated with restoring systems and data, incident management and notification costs, and regulatory, legal and compensation costs.
- **Network security liability**, covering legal and defence costs together with compensation to third parties that incur losses due to a cyber incident against the insured party.
- **Communication and media liability**, covering legal and defence costs together with compensation to injured parties due to digital communications from the insured party resulting in defamation, libel, slander or other harm.
- **Technology disruptions**, providing business interruption cover, together with any technology restoration costs, to the insured party where their operations are disrupted due to technology failure.
- **Cyber extortion**, covering costs to restore data, hardware and software that are compromised due to a ransomware attack.
- **Cyber fraud and theft**, covering financial losses where assets are stolen due to a cyber incident.

The exact cover provided by a policy and limits applied will vary between insurers.

## *Silent cyber comes out of the shadows*

Cyber cover is normally provided through a discrete cyber insurance product or via extensions to an existing liability policy. However, historically, losses arising from cyber incidents have also been covered by standard insurance policies where these policies have not explicitly excluded cyber risks. This coverage is known as silent cyber, or non-affirmative cyber.

**Some insurers have updated their policy wordings to explicitly exclude silent cyber coverages from non-cyber products.**

As the frequency of cyber incidents have increased in recent years, some insurers have updated their policy wordings to **explicitly exclude silent cyber coverages** from non-cyber products. In July 2019, Lloyd's issued a market bulletin mandating clarity of whether cyber is covered in policies, which led to many insurers introducing cyber exclusions or requiring affirmative inclusion of specific covers and pricing explicitly for this. Property covers were first, and most recently PI (professional indemnity) and D&O (directors and officers) covers. Over time, Lloyd's has developed some model exclusion language, which is increasingly in use.

This approach, however, is not consistent across the entire industry, with challenges in defining cyber incidents, and the potential therefore for silent cyber to remain an ongoing issue.

### Hot topics for decision makers

- Compared with more traditional forms of insurance, cyber insurance is a relatively new product covering a rapidly evolving form of risk, which has arisen from technology. This evolution means the exact cover varies between insurers, and so it is critical organisations understand their risks and ensure covers are tailored to their needs.

**37** OECD (2020).

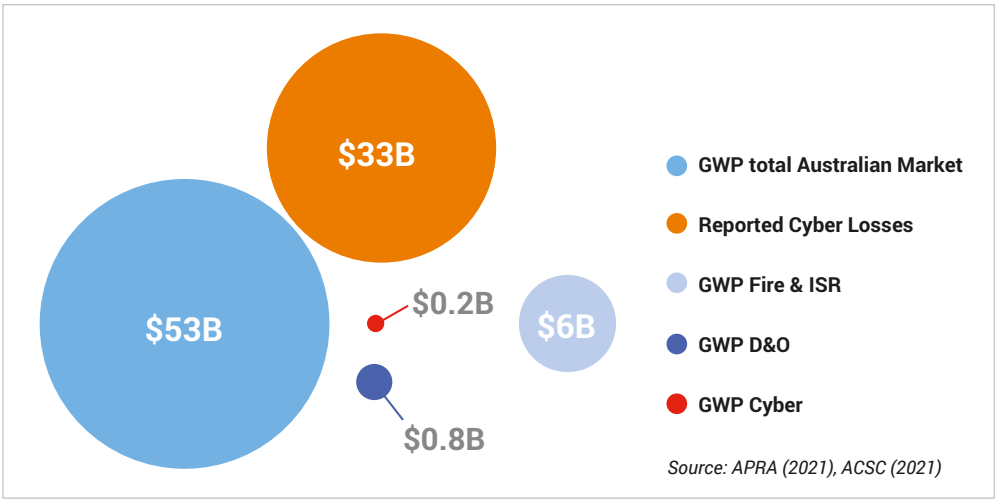
- With silent cyber being removed from non-cyber products, it is imperative for insureds to be certain there is no ambiguity or gaps in cover across their policies.

## *Why size matters – A closer look at the market*

The cyber insurance market has grown significantly over the past decade. However, given its origins as a niche line of insurance cover, it remains a relatively **small component of the overall insurance market**. This, combined with the fact that historically (silent) cyber risks formed part of standard insurance policies, also means it is difficult to accurately estimate the size of the market. Aon estimates that, in 2020, cyber insurance premiums globally were about $9 billion[38]. The size of the Australian market was estimated at more than $110 million, which we expect would be closer to $200 million with recent premium increases. This represents only 0.4% of total gross written premium (GWP) in Australia of $53 billion[39] across all classes. Cyber represents about 4% of the Lloyd's market.

In addition, when compared against reported cyber-related losses of $33 billion in Australia over the past financial year, FY2021, it is clear most losses are uninsured, with cyber insurance premiums representing less than 1% of these losses. This shows that cyber insurance, while growing rapidly, has some way to go yet in reaching its market potential and playing a prominent role in terms of financial compensation for cyber-related losses.

**Figure 3 – Comparative size of cyber insurance market in Australia with other risks**




The diagram shows that the cyber insurance market is a mere speck (see red dot) compared with the total economic loss related to reported cyber incidents in Australia (orange ball). Even if half of this total loss were insured or insurable, it would still swamp every other class of insurance in Australia presently. This includes established classes such as Fire & ISR (industrial special risks) and D&O, which may contain some cyber cover, including silent cyber.

As we mentioned earlier, in Section 3.1, The Geneva Association recognises these "constraints on the private re/insurance sector's capacity to absorb losses from an extreme cyber incident".[40] It has concluded that "…ultimately, some form of government backstop or public-private partnership (PPP) to

**38** Aon Australia (2021).

**39** APRA (n.d.).

**40** Carter, Pain and Enoizi, 2022, p. 5.

finance extreme cyber risks will be needed in order to foster the development of a sustainable private cyber re/insurance market and thereby boost economy-wide resilience."[41]

**Hot topic for decision makers** – Cyber losses, if unaddressed, would be too big a problem for insurers to tackle alone, and stretch the market beyond capacity and resources. Compounding the issue, recent poor returns and significant downside risk have deterred new entrants to the cyber insurance market and led current insurers covering cyber liabilities to reduce their capacity. A key question for discussion is where does accountability lie and who should wear the costs of attacks under various circumstances – businesses, governments, insurers or some combination?

Good cyber hygiene and security will always be key and form the first line of defence.

## 4.2 Cyber insurance – A critical part of robust risk management

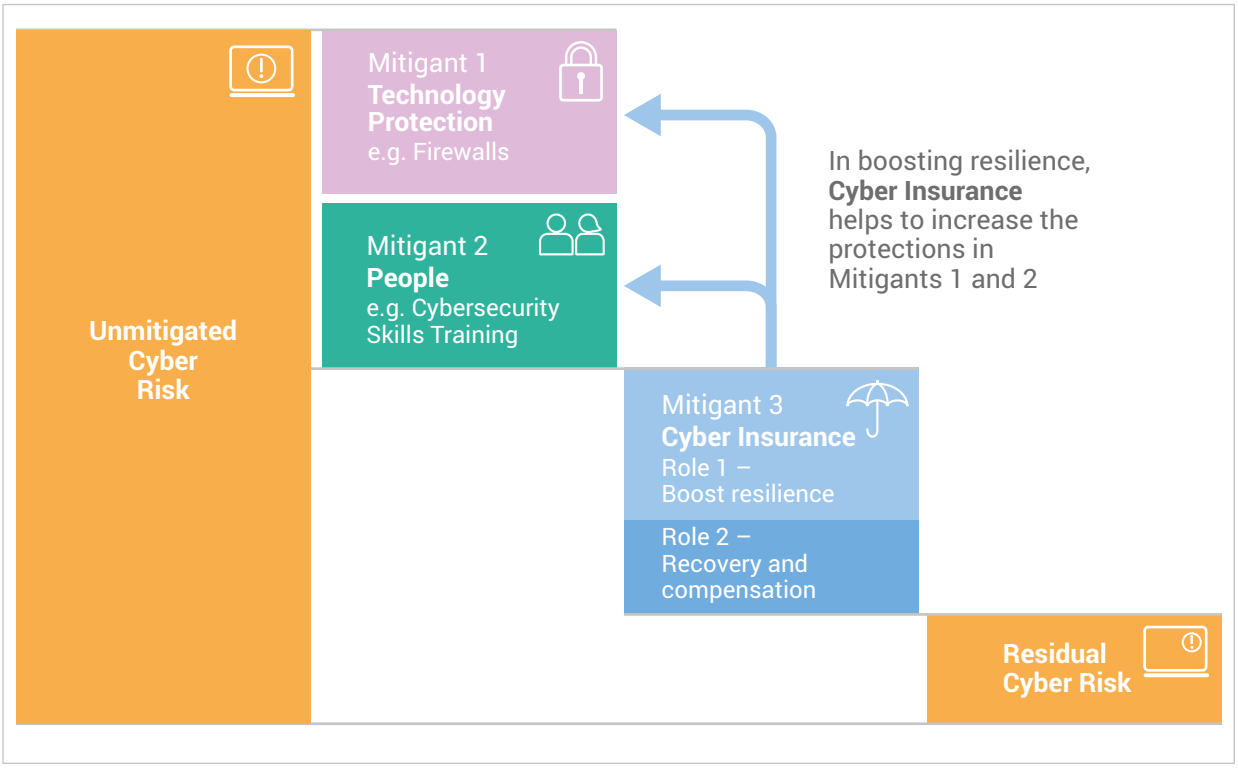
While it forms only a small part of the overall insurance market, cyber insurance has a critical role in an organisation's risk management framework.

Good cyber hygiene and security – which involves a combination of managing physical assets, technology systems, information systems, as well as staff training and education – will always be key and form the first line of defence. As with other traditional forms of insurance, cyber insurance will be required only when threats break through the first line.

Figure 4 below illustrates a conceptual best practice risk management approach to cyber risks and where insurance fits within it.

41 Carter, Pain and Enoizi, 2022, p.7.

**Figure 4 – Conceptual risk management approach to cyber**



We see that cyber insurance plays two key roles in robust risk management, rather than functioning only to provide compensation after an event.

**ROLE 1** – Actively boost the protections in Mitigants 1 and 2, reducing the likelihood and impact of a cyber incident. Insurers can achieve this in three ways.

- **Eligibility**: Insurers will not provide cover where there exist the most egregious gaps in cyber security (thus setting minimum standards).
- **Pricing:** They will charge premiums that reflect the risk (thus providing incentives to mitigate the greatest risks and improve cyber resilience).
- **Insight:** Ideally, the underwriting process will provide organisations with the necessary insights as to what areas they need to improve towards achieving best practice.

**ROLE 2** – Provide recovery and compensation after a cyber incident. This may include aid in managing a cyber event, such as analysis of the cause of the event, restoring systems, and managing public relations and regulatory responses.

## A role in setting guidelines

**Insurance has the potential to establish guidelines and best practice based on responsive underwriting policies and approaches that adapt to the rapidly evolving risks** (that is, identifying weaknesses in the first line of defence and actions for shoring these up). This point is underscored in a Lloyd's study[42], which found that "syndicates demonstrating a more responsive approach to underwriting generally performed better in this class", although the relative immaturity of the sector means there are "variable levels of capability" between syndicates at the moment.

### Calls for minimum standards

In Australia, the Cyber Security Cooperative Research Centre released a report in 2021 on how cyber insurance can help cyber security in Australia[43]. It calls for insurers to set minimum standards of security to encourage an uplift in cyber security for companies that take out cyber insurance. This has the potential to be much more responsive than slowly moving regulations.

Insurers and brokers have had to quickly evolve as underlying claims risk increases for the cyber insurance market. Over the past year, we have seen insurers and brokers significantly strengthen their underwriting processes to increase their understanding of the insureds' cyber security systems. In its 2021 cyber thematic review, Lloyd's noted: "A number of syndicates were able to demonstrate a significant advantage in their underwriting process by using either in house or third-party suppliers to proactively risk assess a potential insured pre-bind … The ability to combine risk management and risk selection into the underwriting process was clear best practice."

### Added insurer scrutiny, but help is at hand

With most insurers increasing their level of underwriting scrutiny, this means that organisations who do not have adequate cyber security may not be able to get cover unless they improve any identified deficits. Along with this extra scrutiny, however, insurers or brokers may also provide additional services to enable organisations to assess their cyber security.

**Some insurers have been refining the wordings in their policies to exclude or limit cover where software patches are not maintained.**

**42** Lloyd's (2021).

**43** Falk and Brown (2021).


Brokers such as Marsh in Australia now provide – even to SMEs – **a cyber security self-assessment tool,** which compares answers provided in a questionnaire to the best practice standards[44].

Aon Australia[45] sets out the various controls now ubiquitously required by the market in order to consider providing cover, including multi-factor authentication, endpoint protection, privilege access management, as well as dedicated cyber business continuity and resiliency plans. More recently, some insurers have been refining the wordings in their policies to exclude or limit cover where software patches are not maintained.

In the US, insurer Coalition has made its **risk management platform freely available to any organisation**, including non-policyholders[46]. The platform assists with controlling risk via attack surface monitoring and cyber risk assessment.

Most cyber policies also include aid in managing a cyber event, which may include undertaking analysis of the cause of the event, restoring systems, and managing public relations and regulatory responses. Insurers will usually have a suite of service providers they may draw upon to assist an insured in response to a cyber incident.

**The appetite for cyber insurance has reduced, with significant reductions over the past year in capacity offered, and increases in premiums.**

### Hot topics for decision makers

- Insurers bring skills in helping customers improve risks as part of the normal underwriting process. Those who lead the market are doing this successfully, with evidence showing these insurers are the most profitable and well supported in limiting losses.
- An insurance approach to assessing risk would focus organisations on the bare minimum needed to obtain protections, with many insurers now requiring organisations to demonstrate at least basic cyber hygiene such as multi-factor authentication. The first year may be hard for them, but processes will be easier to maintain once implemented and will be an important step towards the maturity of cyber security across the nation.
- In the past year, brokers in Australia such as Marsh made vast improvements in helping businesses, including SMEs, to assess their risk score as part of the underwriting process.

**Identifying the gaps** – Market capacity is limited, with restricted coverage terms. The rapidly shifting risks and relative immaturity of the sector mean the capability across insurers is inconsistent and varies widely, with little appetite from potential new entrants.

As for insureds, these organisations will need to be at the top of their game to maintain cover, as a result of increasing insurer scrutiny.

## 4.3 What are the challenges?

Here, we look at the challenges to attaining a vibrant, effective cyber insurance market – from insurer and consumer perspectives.

**44** ISO 27001 or NIST.

**45** Aon Australia (2022).

**46** PRNewswire (2021).

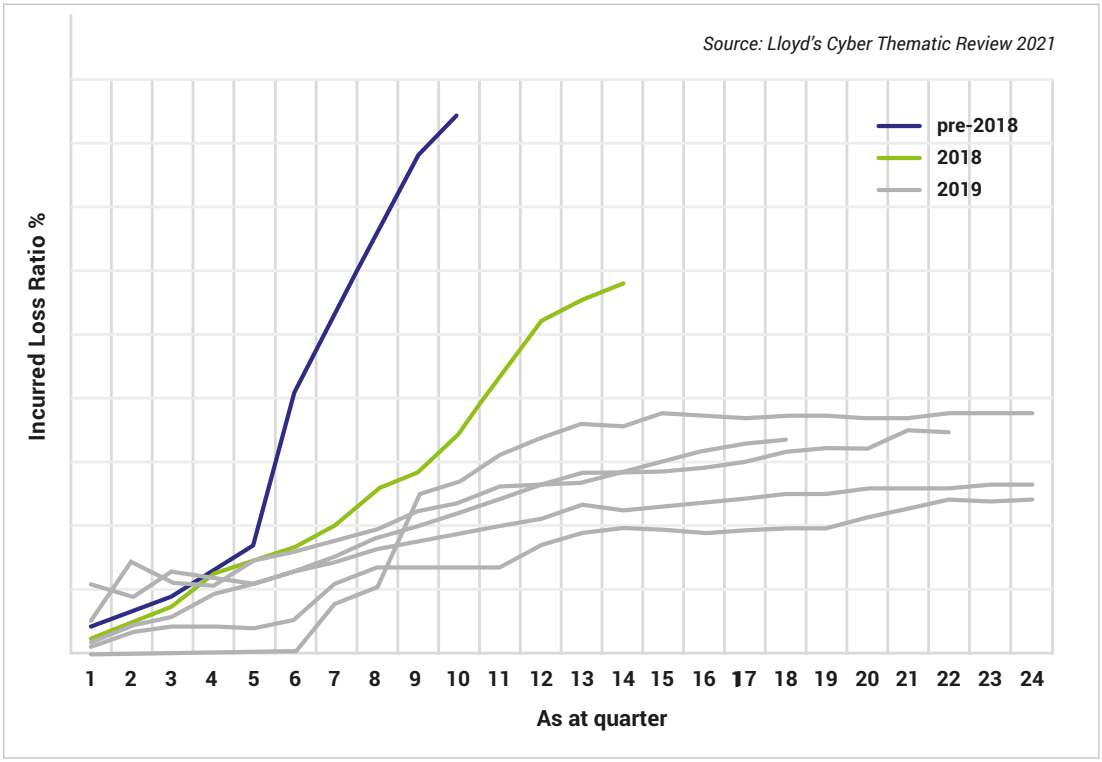
## Insurer challenge 1 – Shortage in capacity

The past two years have been tumultuous and posed serious challenges for the cyber insurance market. As a result, the appetite for this class has reduced, with significant reductions over the past year in capacity offered, and increases in premiums (averaging more than 100% from Q4 2020 to Q4 2021[47]). Reductions in policy limits from $50 million to $10 million are reasonably commonplace, with price increases all the way up the insurance coverage tower and no tapering off in rates at higher levels of cover.

### *Losses, privacy reforms and fines exacerbating the problem*

Among the factors exerting further pressure on capacity, this class experienced losses for the first time in its 20-year history – and the deterioration was sharp, arising mainly from the explosive growth in ransomware. This rise in claims losses is clearly illustrated in the experience for Lloyd's, which writes 20% of the global cyber market, as Figure 5 illustrates.

**Figure 5 – Lloyd's incurred loss development (underwriting years 2013-2019)**



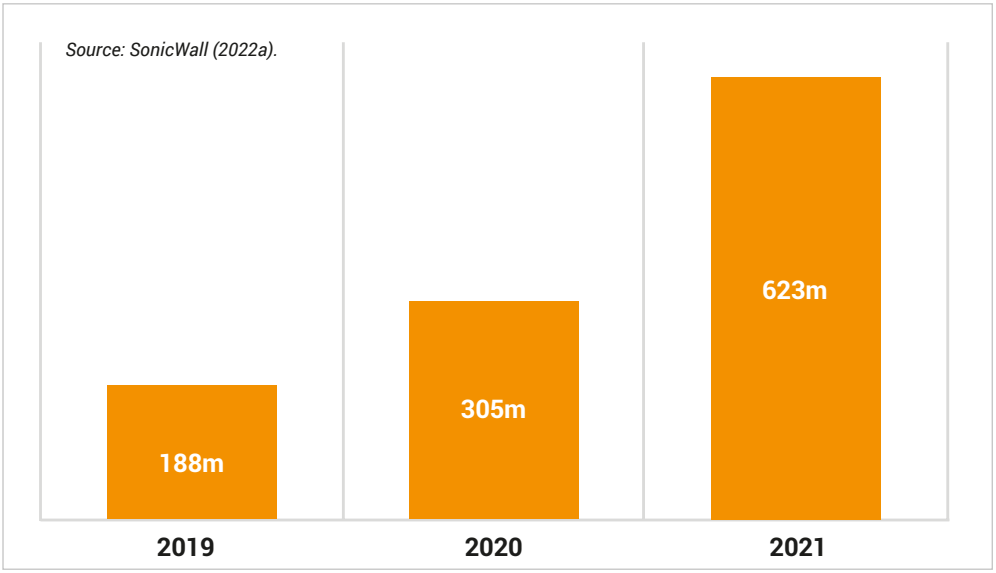

We see that by 2021, the 2019 underwriting year (blue line) already has losses more than twice the year before, (green line) and more than three times that of earlier years (grey lines) at the same stage of development – with no sign of abating.

The Lloyd's review identified ransomware as the most significant driver of the insured cyber losses, although data breaches and network outages were also flagged as material contributors.

Since 2019, ransomware attacks have continued to increase, with 2021seeing the highest number of attacks at more than three times (332%) that of 2019, or 20 attacks every second (Figure 6).

**47** Aon Australia (2022).

**Figure 6 – Number of ransomware attacks globally**




Interestingly, in Australia, the ACSC notes 500 ransomware attacks per year in FY21, up 15% from the previous year – much lower than observed globally. This has to be viewed with caution since reporting of cyber incidents in Australia is not compulsory, other than for those linked with critical infrastructure assets.

Other major factors impacting capacity are the privacy reforms underway to expand definitions of personal information coupled with the significant fine increases for privacy breaches – up to 10% of an organisation's annual domestic turnover, as mentioned in Section 3.1.

### *The aftershocks of loss*

Financial services provider Aon Australia reflects this experience in its 2022 first quarter report[48], confirming "2021 saw the cyber market become the most distressed line of insurance, which corrected at a pace not witnessed for some time". It says to consider providing coverage, the market is now requiring "certain controls", as well as "resiliency plans and a well-articulated submission". Without these, "organisations will struggle to maintain insurance coverage".

The report adds, "Markets are increasingly empowered to walk away from an organisation that cannot adequately explain their security framework and security investment strategy, both historical and future, or to provide terms that are penal or designed to force improved risk management posture."

**Hot topic for decision makers** – Until there is better cyber hygiene to reduce the extraordinary increase in losses directly affecting capacity, someone (i.e. businesses, if insurers are not offering sufficient cover) is still having to pay these mounting costs.

## Insurer challenge 2 – Accumulation risks

One unique feature to cyber insurance risks is that there are no geographical boundaries limiting where a claim can arise. As we have seen recently, a computer virus can spread quickly around the world and result in many

**48** Aon Australia (2022).

companies making a claim under their cyber insurance policy. This is the accumulation challenge for an insurer – the potential for a single event to trigger losses for numerous of its insureds, across business lines and global borders. Some recent examples of large cyber events affecting companies worldwide include the 2020 SolarWinds hack, the 2017 WannaCry and NotPetya attacks. NotPetya affected thousands of companies across 60 countries, with losses of around US$10 billion.

Accumulation risks can arise from several sources.

- **Software vulnerabilities** in common software, such as operating systems, can be exploited and result in a wide spread of attacks globally. The SolarWinds, WannaCry and NotPetya attacks are examples of this accumulation.
- **Attacks on information technology providers** with large user bases. Increasingly, technology is provided via cloud environments. If these services were compromised this could lead to disrupted services for many organisations.
- **Attacks on critical infrastructure providers**, disrupting critical services. This could lead to losses on non-cyber insurance policies, for organisations that suffer losses due to the disruption of these services. Internationally, we have seen the ransomware attack on the Colonial Pipeline in the US, and cyber attacks in the Ukraine, resulting in power cuts.

## *Acts of war*

Cyber war and terror exclusions[49] are a significant aspect of accumulation risks facing the industry. Traditional insurance policies typically exclude war and terror risks, with national pools helping to fill the gaps. The reasoning here is similar in cyber – the risks are potentially large scale and catastrophic, often transcending geographic boundaries and classes of business. From an insurer perspective, excluding war and terror from cyber policies also makes sense.

The challenges are in translating more traditional insurance products into the cyber realm by defining and standardising these exclusions. In particular, as Lloyd's notes in its August 2022 Market Bulletin[50], "… exposure to cyber-attack losses has been an area of market focus in circumstances where the losses arise from attacks sponsored by sovereign states".

This need for updated policy language for cyber risk and cyber war was highlighted in the 2017 NotPetya malware event, attributed to Russian action against Ukraine. US-based pharmaceutical company Merck claimed $1.4 billion against a property insurance policy and courts ruled the claim could not be denied by the insurer based on a war exclusion included in the policy.

Another key challenge – and central to applying war exclusions – is determining the cause and attribution of the source of a cyber event for applying coverage. Mere indications are insufficient to attribute fault 'beyond reasonable doubt', and the diplomatic consequences for flawed attribution may be considerable.

In response, Lloyd's suggests underwriters "need to take account of the possibility that state-backed attacks may occur outside of a war involving physical force" when writing cyber-attack risks. Further, from March 2023,

**The challenges are in translating more traditional insurance products into the cyber realm by defining and standardising war and terror exclusions**

**49** Yeates (2022).

**50** Lloyd's (2022).

any new or renewal of Lloyd's policies must contain a clause with "robust wordings" based on specific requirements excluding liability for losses arising from any state-backed cyber attack, in addition to any war exclusion[51]. This is yet to be tested in the market, but already there are questions about how it may operate in practice. For example, it is unclear what is explicitly meant by "the insurer may rely upon inference which is objectively reasonable" in attributing cyber attacks to a state actor "or those acting on its behalf"[52].

**Hot topics for decision makers**

1. While considerable work has been done and progress made by insurers in trying to understand and model accumulation risk – for example, that attacks tend to cluster by industry sector[53] – the ability to manage the accumulation threat remains the key impediment in establishing a resilient and sustainable market for cyber cover.
2. Aiming to manage accumulation risks, insurers may limit the amount of cover they will offer. As a result, companies may not be able to get the level of cover needed to protect their cyber exposures.
3. Collaboration between government and insurers will be critical towards managing accumulation risk, potentially in government agreeing with insurers on acts of war definitions as well as situations and conditions where pools may help.

## Consumer challenge 1 – How much does insurance really help?

Statistics from the Insurance Council of Australia show that only about 20% of SMEs and 35-70% of larger businesses in Australia have standalone cyber insurance[54]. In New Zealand, this drops to 5%, according to the Australian and New Zealand Institute of Insurance and Finance (ANZIIF)[55]. Given these numbers, it is not surprising that cyber premiums in Australia form less than 1% of reported cyber losses (see earlier Figure 3). The resulting premium hikes, combined with the insurer capacity issues we outlined in Insurer challenge 1, have limited corporates in achieving the level of cover they seek. Boards are now validly questioning the value of buying cyber insurance. Key concerns include:

- Will insurance enable my business to get back on its feet under a serious cyber attack?
- What level of cover is sufficient?
- What risks do I need to cover – data breaches, fines, business interruption, ransomware?
- How well will these products compensate me for impact on brand, reputation, IP and data?

In answering these questions, companies must think carefully about what they want their cyber insurance policy to cover. Two key elements to consider in assessing this are:

- The **sort of events** that could result in a company needing insurance coverage; and
- The **potential total costs** that could result from a claim, and how much of this cost the company is able to absorb. These can include not just financial losses (refunds to customers, fines, and the like), but

**51** Lloyd's (2022).
**52** Lloyd's Market Association (2021).
**53** Hohmann and Wilson (2018).
**54** Insurance Council of Australia (2022).
**55** ANZIIF (2022).

also lost opportunity cost, and 'clean-up' costs such as the forensic investigations and harm to individuals downstream affected by the disruption.

Once companies have been able to ask these questions, they will need to analyse the proposed policy wordings to ensure the policy responds to the scenarios they envisage and also that the level of cover provided is adequate for their circumstances. We highlight the importance of these steps in the following detail, breaking down the costs to insureds in an edited excerpt from a Willis Towers Watson annual report.

### *Cost breakdown – A closer look at cyber insurance in action*

Insurance generally covers only a portion of the total loss from a cyber incident. Insurance adviser Willis Towers Watson publishes an annual report that analyses cyber insurance claims reported from 2013 to December 2019[56]. This report shows that:

1. Insurance covered only **44%** and **37%** of data breach and first party costs respectively. Data breaches were the most frequently reported claims, and had the highest cost, while first party claims were dominated by business interruption and ransomware.
2. Insureds met **54%** and **60%** of data breach and first party costs respectively. Of these:
   - **27%** of data breach claim costs and **36%** of first party claim costs were **below the policy excess limits** and so **were paid by the insureds**.
   - **27%** of data breach claim costs and **24%** of first party claim costs were **not covered by the insurance policies**. Two key reasons for this were **insureds acting without the insurer's consent or using vendors not approved by the insurer.**
3. The remaining **2%-3%** was covered by **third parties**.

## *Cyber attack scenario and stress testing – Where actuaries can help*

Often, the true cost of a cyber attack is not captured by looking at the financial loss alone such as fines and refunds to customers. Other losses can also be significant, including reputational damage, ongoing forensic investigations, lost opportunities, and time needed to rebuild trust with customers and individuals downstream who have been harmed by the disruption.

Here is where actuaries with their skillset are especially valuable.

Actuaries are well placed to build a picture of the range of immediate and longer-term impacts – both financial and non-financial – and stress test the impacts on an organisation's balance sheet or P&L. This insight enables organisations to make robust evidence-based decisions.

In Australia, actuaries have been doing this for regulated financial institutions for many years, using APRA's ICAAP (Internal Capital Adequacy and Assessment Process)[57]. This approach has assisted financial institutions to meet their obligations under a wide range of circumstances. The Board has ownership of the ICAAP.

**Often, the true cost of a cyber attack is not captured by looking at the financial loss alone. Lost opportunities and time needed to rebuild trust with customers are among other significant losses.**

**56** Foster (2020).

**57** APRA (2013).

Scenario analysis and stress tests of potential risk exposures form a key part of this approach. In more recent years, as cyber gains prominence, cyber attacks have featured strongly in the stress tests. We believe this approach can be readily applied to any large corporate, not just financial institutions. It has already been implemented overseas, as we illustrate in the following case study on Tesco in the UK.

## Case study – Stress testing for Tesco in the UK

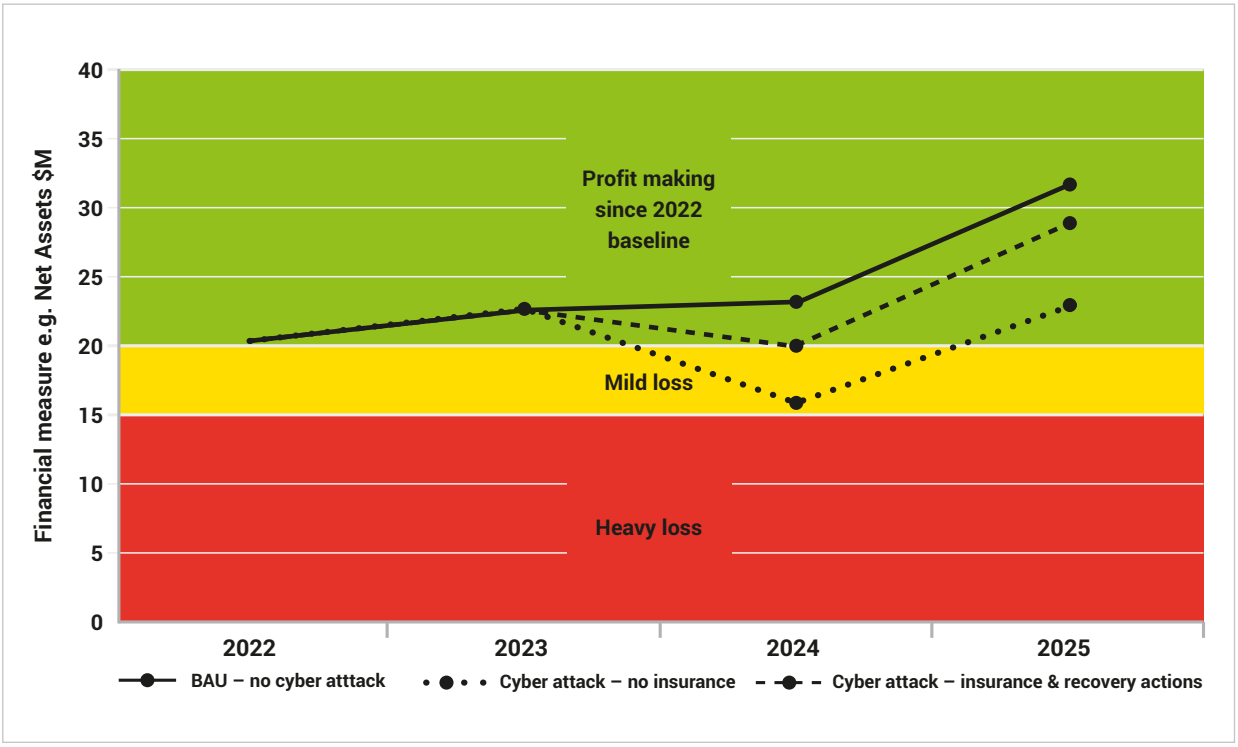
Tesco, which has a market capitalisation of £19.7 billion ($18.3 billion) has not only undertaken these cyber attack stress tests but has published the outcomes in its latest 2022 Annual Report[58]. Tesco's stress test entails a data breach that it assesses could cost it up to £2.4 billion (2% of its revenue) in fines, as well as reputational risk, resulting in a decline in customer sentiment and an adverse trading impact, of high uncertainty in terms of financial impact and the time to recover customer trust. It is worthwhile noting the proposed Privacy Act changes in Australia could expose organisations to penalties of 10% of annual turnover (vs 4% maximum in the UK).

### Australian focus – Sample scenario test

We set out a simple example, in Figure 7, using ICAAP principles, of how the financial position of an organisation may look in the event of a cyber attack causing a data breach. We attempt to put a financial value on the activities required to restore the non-financial risks such as trust, reputation and brand. The projections are shown in a 'business as usual' situation (no cyber attack), a cyber attack (without insurance) and a third scenario, where insurance and other recovery actions are in place – with the impact projected across three years.

58 Why CEOs will (2022).

**Figure 7 – Scenario analysis of cyber incident and effectiveness of insurance**



- **Assumed impact without insurance** – Business reduces by 50% for six months, and one major client terminates its contract. Regulatory fines and IT recovery expenses of $xM, increased spend on communications and brand of $yM, Business Continuity and Disaster Recovery Plans activated.
- **Insurance scenario** – Business interruption and forensic investigation costs met and partial payment of fines under the policy.

In this example, the attack against an uninsured organisation puts its financial position into the amber zone (early warning for significant re-rating by investment markets and creditors, with impact on cost of funding). With cyber insurance in place, the scenario sees the financial position lifting to profitable operating levels (green zone).

**Hot topic for decision makers** – Detailed scenario testing is a vital consideration for organisations wanting to develop robust cyber security frameworks.

Scenario analysis and stress tests have been a part of the approach to ensuring the viability of regulated financial institutions for some years. These can readily be extended to assessing larger companies' viability in the face of a plausible, serious cyber incident, and the value and adequacy of a cyber insurance program in mitigating the impacts for these organisations.

## Consumer challenge 2 – Skills gap in cyber security

Increasing cyber attacks on business and governments, as well as the pandemic, have highlighted a cyber security skills shortage in Australia (see Section 3.1), and around the world.

Working from home has exposed private network and other remote technology vulnerabilities. Globally, 80% of organisations have suffered one or more cyber security breaches during the pandemic, and investigations show these breaches were a result of a lack of cyber security skills and/or awareness. Indeed, most organisations operate a component of legacy systems and fail to maintain the appropriate level of design documents, network insight and comprehension – with expensive stop-gap measures that cause ongoing issues and concerns.

This has far-reaching effects for insurance – not only for insurers but also for organisations seeking cover. As insurers increase their underwriting controls and look to sharpen risk management standards, organisations are having to respond to achieve adequate cyber protection.

A key factor is that organisations cannot find, recruit or retain certified cyber security people. Often security resources are poached for higher paying salaries and better work conditions.  Global leaders indicate that:

- 60% struggle to recruit cyber security talent
- 52% struggle to retain qualified people
- 67% agree that the shortage of qualified cyber security candidates creates additional risks for their organisations.

Increasing cyber attacks on business and governments, as well as the pandemic, have highlighted a cyber security skills shortage in Australia.

Organisations require expert cyber security professionals and, as a result, 76% of organisations say their board of directors now recommends increases in IT and cyber security people.

**Hot topic for decision makers** – With the high demand on cyber security personnel from all quarters (including government – see Section 3.1), collaboration is needed between government, businesses and insurers to recruit and build up the right skillsets, deploy them to best effect and avoid detrimental competition for these resources.

In the business world there is some hesitation in taking out cyber insurance.

## Consumer challenge 3 – Cyber hesitancy and misconceptions

While cyber issues are top of mind for large corporates, there are several issues often expressed in the business world leading to some hesitation in taking out cyber insurance – but are these beliefs well founded? We explore some of the key issues and concerns.

**Aren't cyber insurers just 'shadow directors'?**

One common issue centres on Boards worrying about relinquishing control and the insurer becoming 'shadow directors' in a cyber event. From our discussions and research for this paper, this appears to be a misconception.

In particular, we highlight the responses to this question from two parties closely involved with executing the detail of cyber policies and when claims occur:

- Clyde & Co, which provides cyber risk services, including incident response
- Marsh, one of Australia's major cyber insurance brokers.

John Moran, who leads Clyde & Co's cyber incident response team in Australia, says: "It's a myth. While insurers may provide access to additional vendors in the event of a claim, they do not have the power to take over the management of the claim against the wishes of the insured – for instance, the Board are involved in key decisions around payment of a ransom, communications to stakeholders, or disclosure of an incident to the ASX. Where additional vendors are recommended by the insurer, the relationship will be a direct one between the vendor and the insured – the insurer may simply end up paying the bill. As with other classes of insurance, the insured is required to keep the insurer updated and involved in the claim."

> "It's a myth … insurers … do not have the power to take over the management of the claim against the wishes of the insured."
>
> John Moran, Clyde & Co incident response lead

Hannah Morgans, Growth Leader – Cyber Practice, Marsh Australia, says: "The policy is set up to support the board, rather than hinder. The primary objective of the initial incident response vendors is to provide support to existing technology, legal, risk and executive teams. Everyone has their day-to-day job and responsibilities. Management or running of a company doesn't stop because of a cyber event. If anything, effective management becomes more critical. Cyber insurance provides access to that additional layer of specialist

services that brings extra 'hands on deck' to respond swiftly to an incident and guide the business to recovery, with as minimal impact as possible – financially, operationally and reputationally."

**Hot topic for decision makers** – One common misconception is that insurers can take over the management of a cyber insurance claim[59]. This is possibly an impediment for large companies that choose not to take up insurance.

### *Will having cyber insurance make my business a bigger target?*

Some organisations may choose not to take out cyber insurance in the belief that having the insurance would make their company a bigger cyber target. This is not helped by commentary such as the following quote by the ReVil ransomware gang, when asked whether their operators target organisations that have cyber insurance[60], "Yes, this is one of the tastiest morsels. Especially to hack the insurers first – to get their customer base and work in a targeted way from there. And after you go through the list, then hit the insurer themselves."

> "… this is one of the tastiest morsels. Especially to hack the insurers first – to get their customer base and work in a targeted way from there … then hit the insurer themselves."
>
> ReVil ransomware gang

The audacity of this attitude may well discourage organisations further, but it is worth pausing to reflect on the consequences of having no insurance in place to assist either in mitigating the impacts of a cyber attack or restoring any loss of income to the business. It is also important to note that not having insurance does not remove the potential to be targeted. Ultimately, any business that utilises technology and/or has access to confidential/sensitive/valuable data will be at risk of being a target.

Akin to kidnap and ransom insurance, we believe the insurance should be purchased if it forms part of an organisation's risk management strategy – but is good practice to keep the policy in a secure location and not publicise its details.

**Hot topic for decision makers** – The right question to ask in deciding whether to take out cyber insurance may be: which is the bigger risk and more detrimental to your organisation, the elevated possibility of attack with insurance in place or sustaining an attack without the insurer in your corner?

### It won't happen to me – I'm an SME

As we note in Section 2.3, attacks are increasingly shifting towards smaller firms, which are exposed as easier targets, and where there is a lesser risk of repercussions. But only 20% of SMEs currently have cyber insurance.

A key reason for this is a lack of awareness of cyber risks and engagement with available cyber educational materials. This is exacerbated by the


Ultimately, any business that utilises technology and/or has access to confidential/sensitive/valuable data will be at risk of being a target.

**59** Falk and Brown (2021).

**60** Smilyanets (2021).

perception that 'it won't be me' or that their business may be too small or inconsequential for threat actors to bother targeting.

**Cyber insurance has the potential not only for financial recompense but also in safeguarding a company's reputation.**

We spoke with Natalie Fisher[61], whose firm of four people, Fisher Conveyancing, was subject to a phishing scam that redirected her emails and enabled the hacker to impersonate her in email correspondence instructing clients to transfer monies intended for a property purchase to the hacker's account. She says:

> "If I didn't have this [cyber insurance] policy, it would have ruined me. Not just financially but my reputation, everything. You can't not have it."
>
> Natalie Fisher, Fisher Conveyancing

The insurance covered all refunds to her clients, the forensic investigations and associated costs. "I was lucky that a mentor encouraged me to get cyber insurance a few months earlier," Natalie adds. "There's little awareness of cyber insurance among small business. I agree there needs to be more education."

It is interesting to note that cyber insurance not only assisted in providing Natalie Fisher with financial recompense but also in upholding her company's reputation.

**Hot topic for decision makers** – There is a gap to address in ensuring SMEs receive better education on cyber risks and insurance. This will help in gaining a fuller understanding of the potential impacts to their business and reputation, and the role of cyber insurance in limiting those risks.

**61** Grieve (2022).

# Conclusion

5

## Cyber risks – a perpetual game of catch-up

In this paper, we have looked at the growing cyber risk and the widening impact on organisations of different types and sizes. Despite an increasing cyber spend by both government and business, government entities are a long way off baseline standards of cyber security. As well, many businesses are behind in managing cyber resilience in the face of rapidly shifting risks, and support for SMEs is inconsistent, with low awareness of educational materials.

## The role of cyber insurance in setting best practice standards for cyber resilience

We investigated the role of cyber insurance in setting best practice standards for cyber resilience, as part of a robust risk management framework. Beyond reimbursement, we found the best underwriting practices have the potential to actively help increase cyber protections and reduce the likelihood and impact of a cyber incident.

## Gaps to a sustainable, effective insurance market

However, in order for cyber insurance to influence best practice in a major way, there are several gaps that need to be addressed by government, business and insurers. Adding to these challenges are escalating cyber losses that have reduced appetite for this class, significant shortage of capacity to provide the levels of protection needed across the market, and premium hikes in the double/triple digits over the past two years. Among the key gaps are:

- **A skills gap and severe shortage of qualified cyber security personnel,** with no established framework for leadership in cyber security – 60% of global leaders have indicated a struggle to recruit cyber security talent
- **A shortage of Board directors and executive management** with a strong understanding of cyber risks and insurance – and the consideration of cyber not just as a technological risk but a business risk within a comprehensive risk framework
- **A need for better engagement of SMEs** in education on cyber risks, in an environment where attacks are increasingly shifting towards smaller companies
- **Achieving sufficient capacity and profitability in the market,** with reduced appetite for this class following the losses over the past two years
- **Management of the accumulation risk for insurers,** with the potential for a single event to trigger numerous losses, across business lines and global borders – and challenges in implementing cyber acts of war and terrorism exclusions

**For cyber insurance to influence best practice in a major way, there are several gaps that need to be addressed by government, business and insurers.**

- **Cyber hesitancy in seeking the right insurance solutions**, from misconceptions such as the fear of relinquishing control or being a bigger target.

While there have been significant gains in addressing many of these areas, the issues are too vast to be solved in isolation and collaboration between all stakeholders – government, business and insurers – will be critical towards creating a resilient and sustainable insurance market.

## Collaboration – Charting the path to 'gold standard'

Each party brings existing skills, and established frameworks and processes that can be drawn upon to great effect collectively. Some examples of this include:

- **Scenario analyses and stress tests of potential risk exposures**, including cyber risks, that form a key part of the ICAAP approach instituted by APRA. This framework has served to ensure the financial viability and resilience of financial services organisations for almost 10 years. It is an area where actuaries have been involved for many years, and can be readily adapted to any large corporate, outside of just financial institutions
- **Government and insurers partnering towards managing accumulation risks**, including, for example, discourse around consistent acts of war definitions, as well as situations and conditions where pools may help
- **Government, businesses and insurers working together to bolster skills**, with the high demand on cyber security personnel from all quarters. By collaboratively creating pathways to recruit and build up the right skillsets – for example programs encouraging insurers to take on people and provide tactical training within their businesses – these organisations can deploy initiatives to best effect and avoid detrimental competition for these resources

  Another area with further collaborative potential is the increasing regulatory obligations and penal environment imposing fines and penalties for cyber breaches (the stick). An opportunity exists for this to better align with building up the structures needed for a coordinated focus on research and innovation, and to develop the cyber security expertise to fix issues and lift standards (the carrot).

## Opportunity amid uncertainty

We are undoubtedly living in uncertain times that are stretching our collective resilience. In this environment, increasing cyber attacks by technically agile criminals able to react and evolve their tactics with ease are having catastrophic effects for government, businesses and people across the globe.

In meeting the challenges, cyber insurance has great potential to play a key role as part of robust risk management. At the centre of its success will be collaboration between all stakeholders and a collective use of skills in creating an effective sustainable insurance market and uplifting the cyber security of the nation as a whole.

**Cyber security issues are too vast to be solved in isolation and collaboration between all stakeholders is needed.**

**We are undoubtedly living in uncertain times, in which increasing cyber attacks by technically agile cyber criminals are having catastrophic effects for government, businesses and people across the globe.**

# References


Agarwal, H. (2016, May 27). *Kevin Mitnick- From Being Hunted By The FBI To Working Alongside Them*. appknox. https://www.appknox.com/blog/kevin-mitnick

Airmic. (2021). *Our world has changed forever – The Airmic Perspective - Annual survey 2021*. https://www.airmic.com/system/files/technical-documents/Airmic%20Annual%20Survey%202021_main%20report.pdf

ANZIIF. (2022, August 10). *New Zealand Cyber Market Insights* [Webinar]. https://anziif.com/professional-development/events/anziif-webinar-new-zealand-cyber-market-insights

Aon Australia. (2021). *Cyber Insurance Market Insights Q1 2021*. https://aoninsights.com.au/cyber-insurance-market-insights-q1-2021/

Aon Australia. (2022). *Cyber Insurance Market Insights Q1 2022*. https://aoninsights.com.au/cyber-insurance-market-insights-q1-2022/

Australian Cyber Security Centre (ACSC). (2021a). *Cyber Security and Australian Small Businesses: Results from the Australian Cyber Security Centre Small Business Survey*. https://www.cyber.gov.au/sites/default/files/2021-05/Cyber%20Security%20and%20Australian%20Small%20Businesses%20Survey%20Results%20-%2020201130.pdf

Australian Cyber Security Centre (ACSC). (2021b). *ACSC Annual Cyber Threat Report* – 1 July 2020 to 30 June 2021. https://www.cyber.gov.au/sites/default/files/2021-09/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf

Australian Prudential Regulation Authority (APRA). (n.d.) *Quarterly general insurance performance statistics* [Dataset]. https://www.apra.gov.au/quarterly-general-insurance-statistics

Australian Prudential Regulation Authority (APRA). (2013). *CPG 110 Internal Capital Adequacy Assessment Process and Supervisory Review*. https://www.apra.gov.au/industries/2/standards

Bourlioufas, N. (2022, May 4). 'Cyber shortages drive higher pay and new demand for education'. *Australian Financial Review*. https://www.afr.com/work-and-careers/education/cyber-shortages-drive-higher-pay-and-new-demand-for-education-20220503-p5ai28

Carter, R.A., Pain, D. and Enoizi, J. (2022). (2022). *Insuring Hostile Cyber Activity: In search of sustainable solutions*. The Geneva Association. https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cybersolutions_web.pdf

Commonwealth of Australia. (2020). *Australia's Cyber Security Strategy 2020*. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

Commonwealth of Australia. (2022). *Budget 2021-22*. https://archive.budget.gov.au/2021-22/index.htm

Coverware. (2022, February 3). *Law enforcement pressure forces ransomware groups to refine tactics in Q4 2021*. https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021

CyberCX. (2022). *Upskilling and expanding the Ausrtalia cyber security workforce*. https://cybercx.com.au/cyber-skills-report/

Department of Home Affairs. (n.d.a). *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*. https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems

Department of Home Affairs. (n.d.b). *Strengthening Australia's cyber security regulations and incentives*. https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-regulations-incentives

Falk, R. and Brown, A. (2021). *Underwritten or Oversold? How cyber insurance can hinder (or help) cyber security in Australia.* Cyber Security Cooperative Research Centre. https://cybersecuritycrc.org.au/sites/default/files/2021-10/Underwritten%20or%20oversold%20%20-%20DV.pdf

Fortinet. (2022). *2022 Cybersecurity Skills Gap*. https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf

Foster, P. (2020). *Cyber claims analysis report: Turning data into insight*. Willis Towers Watson. https://www.willistowerswatson.com/en-AU/Insights/2020/07/cyber-claims-analysis-report

Glover, C. (2021, September 21). *US government ready to experiment with banning ransomware payments*. Techmonitor. https://techmonitor.ai/technology/cybersecurity/banning-ransomware-payments-us-joe-biden

Grieve, C. (2022, January 5). 'You can't not have it': Companies turn to cyber insurance as hackers rise.' *The Sydney Morning Herald*. https://www.smh.com.au/business/banking-and-finance/you-can-t-not-have-it-companies-turn-to-cyber-insurance-as-hackers-rise-20211215-p59hpn.html

Hack, P. and Wu, Z. (2021, November 12). *'We wait because we know you.' Inside the ransomware negotiation economics*. nccgroup. https://research.nccgroup.com/2021/11/12/we-wait-because-we-know-you-inside-the-ransomware-negotiation-economics/

Hohmann, D.M. and Wilson, S. (2018). *Advancing Accumulation Risk Management in Cyber Insurance: Prerequisites for the development of a sustainable cyber risk insurance market*. The Geneva Association. https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/report_advancing_accumulation_risk_management_in_cyber_insurance_0.pdf

Insurance Council of Australia. (2022). *Cyber Insurance: Protecting our way of life, in a digital world*. https://insurancecouncil.com.au/wp-content/uploads/2022/03/Cyber-Insurance_March2022-final.pdf

International Organization for Standardization (ISO). (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. https://www.iso.org/standard/54534.html

(ISC)². (n.d.). *ISC² Cybersecurity Workforce Study, 2021*. https://www.isc2.org/Research/Workforce-Study#

isPartners. (2022). *Why Is ISO Certification More Popular Among U.S. Businesses?* https://www.ispartnersllc.com/blog/becoming-iso-27001-certified/

Leibel, A. (Host). (n.d.). *Episode 25: In case you missed it: are you prepared for a cyber incident?* [Audio podcast]. The Secure Board. https://www.thesecureboard.com/podcast/e25

Lloyd's. (2022, August 16). *Market Bulletin: State backed cyber-attack exclusions*. https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf

Lloyd's Market Association. (2021, November 25). *Cyber War and Cyber Operation Exclusion Clauses*. https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx

Lloyd's Cyber Thematic Review 2021.

OECD. (2020). *Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation*. www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf

OpenText Content Server. (n.d.). *09. ISO Survey of certifications to management system standards – Full results*. https://isotc.iso.org/livelink/

PRNewswire. (2021, May 18). *Leading Cyber Insurance Provider, Coalition, Launches Free Risk Management Platform to Help Organizations Combat Ransomware and Cyber Risk.* https://www.prnewswire.com/news-releases/leading-cyber-insurance-provider-coalition-launches-free-risk-management-platform-to-help-organizations-combat-ransomware-and-cyber-risk-301293410.html

Rains, T. (2020). *Cybersecurity Threats, Malware Trends, and Strategies - Mitigate exploits, malware, phishing, and other social engineering attacks*. Packt.

Rittel, H. W. J. and Weber, M. M. (1973). Dilemmas in a General Theory of Planning. *Policy Sciences*, *4*(2), 155-169 http://www.jstor.org/stable/4531523

Sadler, D. (2021, June 10). *Government to mandate Essential Eight cyber controls*. InnovationAus.com. https://www.innovationaus.com/govt-to-mandate-essential-eight-cyber-controls/

Smilyanets, D. (2021, March 16). *'I scrounged through the trash heaps … now I'm a millionaire:' An interview with REvil's Unknown.* The Record. https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/

SonicWall. (2022a). *2022 SonicWall Cyber Threat Report.* https://www.sonicwall.com/medialibrary/en/white-paper/2022-sonicwall-cyber-threat-report.pdf

SonicWall. (2022b). *Mid-Year Update: 2022 SonicWall Cyber Threat Report*. https://www.sonicwall.com/2022-cyber-threat-report/

Standage, T. and Stevenson, S. (Hosts). (2018, October 3). *Human Insecurity: The French telegraph system was hacked in 1834. What does the incident teach us about modern-day network security?* S1E5. [Audio podcast]. Slate. https://slate.com/technology/2018/10/what-an-1834-hack-of-the-french-telegraph-system-can-teach-us-about-modern-day-network-security.html

The Treasury. (2021). *Terrorism Insurance Act Review*. https://treasury.gov.au/sites/default/files/2021-12/p2021-230249-review-final-report.pdf

Tunggal, A.T. (2022, June 1). *What is Cybersecurity Risk? A Thorough Definition*. UpGuard. https://www.upguard.com/blog/cybersecurity-risk

*Why CEOs will take notice of Tesco's cyberattack stress test*. (2022, May 16). Verdict. https://www.verdict.co.uk/tescos-cybersecurity-test/

World Economic Forum. (2022). *The Global Risks Report 2022*. 17th Edition. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

WTW and Clyde & Co. (2022). *Directors' Liability Survey 2022*. https://www.wtwco.com/en-AU/Insights/2022/04/d-and-o-liability-survey-2022

Yeates, P. (2022, July 22). 'Cyber insurance and war'. *Actuaries Digital*. https://www.actuaries.digital/2022/07/22/cyber-insurance-and-war/

**Institute of Actuaries of Australia**
ABN 69 000 423 6546

Level 2, 50 Carrington Street
Sydney NSW Australia 2000
**t** +61 (0) 2 9239 6100
**e** actuaries@actuaries.asn.au
**w** www.actuaries.asn.au