CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

Underwritten or Oversold?

How cyber insurance can hinder (or help) cyber security in Australia

By Rachael Falk and Anne-Louise Brown

cybersecuritycrc.org.au

ABOUT THE AUTHORS:

Rachael Falk, CEO, Cyber Security Cooperative Research Centre

Rachael Falk commenced as the Chief Executive Officer of the Cyber Security Cooperative Research Centre in May 2018, where she leads a cutting-edge program of cyber security research collaboration between government, industry and research institutions. Rachael is a member of the Federal Government's Industry Advisory Committee to help guide the implementation of *Australia's Cyber Security Strategy 2020*. She has a strong background in commercial law and cyber security, having practiced both in top tier law firms and as in-house lawyer at Telstra Corporation Limited. From 2012, Rachael held variety of cyber security roles at Telstra and was the company's first General Manager of Cyber Influence. She is co-author of *Exfiltrate, encrypt, extort: The global rise of ransomware and Australia's policy options*.

Anne-Louise Brown, Director of Corporate Affairs and Policy, Cyber Security Cooperative Research Centre

Anne-Louise Brown is the Director of Corporate Affairs and Policy at the Cyber Security Cooperative Research Centre. Anne-Louise is a former journalist with a passion for developing innovative and creative public policy solutions in the cyber security space. She is fascinated by the nexus between law, human behaviour and cyber security and how public policy can keep pace with rapidly evolving technology. Leveraging policy ideas that can make a real-world difference is Anne-Louise's key aim, as is explaining complex concepts in a way accessible to all people. She is co-author of *Exfiltrate, encrypt, extort: The global rise of ransomware and Australia's policy options.*

INTRODUCTION

Data is valuable. Therefore, it is unsurprising the insurance market has capitalised on this precious commodity – one wrapped up in layers of regulation and vital for the ability of almost all organisations to operate effectively.

In the world of insurance, cyber policies are a relatively new offering. In Australia, the market remains relatively immature, though it is growing, while in the United States, cyber insurance is far more established, with the first policies developed in the 1990s.[1] But a prudent approach is required, because when it comes to cyber insurance, while there are positives, there are also pitfalls and perils. And, most importantly, cyber insurance is not a cyber security silver bullet. It should be viewed as a tool – part of a holistic cyber security strategy – that helps in recovery and remediation after a cyber incident. It is a gap filler. Taking out cyber insurance should never be viewed as a cyber security strategy in and of itself. Like any cyber security product, it is part of a bigger picture and process.

This policy paper explores a number of issues related cyber insurance, with a focus on how it can hinder and help cyber security uplift across the Australian economy. It takes into account the US experience, where the industry is currently in a state of flux, and makes four key policy recommendations to help ensure cyber insurance plays a positive role in Australia.

These recommendations relate to: insurers making ransom or extortion payments as part of any cyber insurance offering; greater clarity regarding the management of cyber insurance underwriting risk and clear articulation of what is and is not covered by cyber insurance; the development of a *Cyber Security Checklist* for SMEs by insurers; and opportunities for insurers to partner with other service providers to offer 'bundled packages' for cyber security uplift.

1. Cyber Insurance History | ProWriters (prowritersins.com)

WHAT IS CYBER INSURANCE?

Cyber insurance is very much a product of the 21st century, created as a response to issues that have arisen through the predominance of the internet and the booming digital economy. Almost all modern organisations, no matter how large or how small, rely on connectivity to operate. Many are also duty-bound to protect the personal information of citizens using their services. Vast repositories of valuable data are stored online, and the intrinsic interconnectedness of the digital age means organisations fundamentally rely on online systems for business continuity. Hence, a cyber breach or incident has the potential to be very costly.

Like traditional insurance policies, cyber insurance generally covers first and third-party losses. First party loss refers to losses incurred directly by the insured. Third party loss relates to losses experienced by the insured as a result of a cyber incident that impacted one or multiple third parties, for which the insured is liable.

Policies generally cover a range of costs,[2] including those related to:

Business Interruption

Incident Response

System Remediation

Legal Representation

Victim Compensation

Regulatory Infringements

Theft or Fraud

Extortion or Ransom Demands

In the past, cyber insurance was often purchased as an 'add-on' to standard business liability insurances. However, as the risks posed by cyber threats have increased and evolved, there has a been a shift to establish cyber risk as a stand-alone issue and, subsequently, a stand-alone insurance product. Therefore, organisations seeking cyber-specific coverage are required to take out a cyber insurance policy.

2. Cyber insurance - key issues for insurers - Taylor Fry

SNAPSHOT: CYBER INSURANCE IN THE UNITED STATES

The US was the first nation to embrace cyber insurance and, as previously mentioned, was where the first policies were developed in the 1990s. Since then, the industry has evolved to become big business, with the value of premiums now totalling about US$5 billion annually.[3] A recent global report into the cyber insurance market found in 2018, 34 per cent of US organisations had standalone cyber insurance, with risk transfer the key reason for taking out such a policy.[4] However, research into the underwriting processes of US cyber insurance policies also indicates a lot of variance.[5] A 2018 study, which analysed 235 policies from New York, Pennsylvania and California, reported "a surprising variation in the sophistication (or lack thereof) of the equations and metrics used to price premiums".[6]

The US market is also under pressure. The global epidemic of ransomware attacks, which have amped up significantly over the past year, has had huge ramifications for the US cyber insurance market, with predictions premiums will increase 20-30 per cent year-on-year.[7] This is forcing a reassessment of cyber insurance policies in the US, where the 'golden rule' of insurance – that the premiums of the many pay for the claims of a few – is being severely tested. As it stands, many policies cover a range of ransomware-related costs, most controversially extortion payments. And in the US over the past year, demand has begun to outstrip supply. It has been estimated ransomware now accounts for 75 per cent of all cyber insurance claims in the US, up from 55 per cent in 2016,[8] with the percentage increase in claims exceeding that of premiums. Ultimately, this has placed the future of the industry in a tenuous position. In the short-term, it has resulted in insurers offering more limited coverage. However, some predict the situation is untenable and that many insurers will withdraw from the market altogether.[9]

The need for a re-evaluation of the US cyber insurance market was highlighted on 25 August this year, when US President Joe Biden met with private sector leaders as part of his high-profile whole-of-nation initiative to lift cyber security.[10] At the meeting two cyber insurance companies, Resilience and Coalition, announced new measures they would implement to bolster cyber security. Resilience said it would now require policy holders to "meet a threshold of cyber security best practice as a condition of receiving coverage", and Coalition announced it would make its cyber security assessment and monitoring platform freely available to any organisation.[11] The steps being taken by these insurers illustrate the important role cyber insurance can play in supporting cyber uplift, through simple measures like setting baseline security standards and providing security assessments.

3. The Next Five Years: Cyber Insurance Predictions Through 2025 (forbes.com)
4. Cyber insurance - statistics & facts | Statista
5. Romanosky et al, Content analysis of cyber insurance policies: How do carriers price cyber risk?, Journal of Cyber Security. 2019
6. Ibid 5. P18
7. Ibid 3
8. Cyber insurance market encounters 'crisis moment' as ransomware costs pile up - CyberScoop
9. Ibid 8
10. FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity | The White House
11. Ibid 10

AUSTRALIA'S CYBER INSURANCE MARKET

While still relatively immature, Australia's cyber insurance market has expanded significantly over the past several years.[12] However, the market remains quite opaque. Given the lack of transparency regarding cyber insurance policies in Australia it is currently difficult to ascertain just how many exist and what these policies cover or exclude. However, recent steps by the insurance regulator, the Australian Prudential Regulation Authority (APRA), should make information about Australian cyber insurance policies more accessible. It will also provide greater insight into the number of organisations that have taken out cyber insurance, which remains unclear.

In late 2020, APRA began a consultation regarding the collection of cyber insurance and management liability data in the National Claims and Policies Database (NCPD).[13] As a result, the collection of this data, which was previously aggregated with data on other product classes, will become mandatory at the end of 2021. The APRA consultation notice states: "Given the recent growth in cyber insurance products and the limited availability of data to assess performance and make pricing decisions for these two products, APRA now proposes to include cyber insurance and management liability in the NCPD data collection as standalone categories".[14]

GREATER TRANSPARENCY

As noted, Australian cyber insurance policies remain enigmatic. There is little publicly available information regarding the inclusions and exclusions provided by specific policies. Furthermore, while it is well known standard exclusions are applied for losses occurring as the result of an act of terror or war (state-based or state-sponsored cyber incident), it remains significantly vague in a cyber context as to what specific events this may apply to. This is made all the more difficult due to the complexities and time taken to attribute a cyber incident.

This lack of clarity was highlighted at a recent hearing of the House of Representatives' Standing Committee on Economics,[15] where Insurance Australia Group's CEO Nick Hawkins stated, in relation to an insurer's liability for ransom payment: "If part of the cost ends up being some sort of cost to the negotiation and consultants and even potentially a ransom, my understanding is that that is of the coverage. However, the way it also works, and I think this is standard in the industry, is that none of those payments can contravene any laws. So, if there is any sort of suggestion that payments are money laundering or if there are any acts or laws in the country that don't allow it or that you are contravening by making this sort of payment, then that is an exclusion, and that payment is not allowed to be made".[16]

This uncertainty is exacerbated by 'silent cyber' – cyber risk that is not explicitly included or excluded in insurance policies.[17] As a result, organisations may be under the assumption they are adequately covered for cyber risks when, in reality, this is far from certain.

This uncertainty, which is a global phenomenon, prompted the OECD to release its *Encouraging Clarity in Cyber Insurance Coverage* report in 2020. The report states: "Insurance regulators and supervisors should encourage the harmonisation of coverage definitions and exclusions applied to cyber risks and monitor the level of claims disputes that arise due to ambiguous policy language".[18] Furthermore, the report signalled the important role public policy and regulation can play in providing clarity, highlighting steps taken by the UK's Prudential Regulation Authority (PRA). The PRA has provided a guidance outlining its expectations regarding the management of cyber insurance underwriting risk, which recommends companies offer explicit cover for cyber risks or clearly articulate exclusions.[19]

12. Cyber-Insurance-Market-Insights-Q1-2021-Final.pdf (aoninsights.com.au)
13. Consultation on collection of cyber insurance and management of liability data in the NCPD (apra.gov.au)
14. Ibid 13
15. Standing Committee on Economics_2021_06_25_8906_Official.pdf;fileType=application/pdf (aph.gov.au)
16. Ibid 15. P50
17. Silent Cyber: What It is and How You Can Cover Cyber Perils (marsh.com)
18. Encouraging Clarity in Cyber Insurance Coverage (oecd.org), P25
19. Ibid 18. P12

MURKY WATER - ACT OF WAR EXEMPTIONS

The 2017 NotPetya malware attack was devastating, predicted to have amassed global losses of up to US$10 billion.[20] It was also a wake-up call for many large organisations impacted by NotPetya, which believed their insurance would cover damages, with the New York Times declaring the attack as "a watershed moment for the insurance industry".[21] And the ramifications are still being felt today.

NotPetya was attributed to the Russian government, which was targeting the Ukraine. But the collateral damage was massive – impacting the companies including US pharma giant Merck, global confectionary company Mondalez (with Hobart's Cadbury factory brought to a standstill), and logistics company FedEx. However, cyber insurance covered just three per cent of the global damage.[22] This has led to years of ongoing litigation brought by Merck and Mondalez against their insurers, who invoked 'act of war' exemptions to insurance policies and, hence, did not pay damages.[23] Merck continues to seek US$1.3 billion in damages and Mondalez $100,000,000.[24]

The OECD has noted "the involvement of politically motivated actors in perpetrating cyber attacks adds a further layer of complexity to questions around where (or whether) cyber losses are covered".[25] Furthermore, as previously mentioned, attribution of cyber attacks can be complex, especially as it comes to sophisticated state-based actors. The difficulty of cyber attribution has been acknowledged by the US Office of the Director of Intelligence which, in its *A Guide to Cyber Attribution*, states: "No simple technical process or automated solution for determining responsibility for cyber operations exists. The painstaking work in many cases requires weeks or months of analysing intelligence and forensics to assess culpability".[26]

WHAT ABOUT REINSURANCE?

Reinsurance, put simply, is insurance that insurance companies take out to guarantee the polices sold to consumers as a risk mitigation measure.[27] Recent volatility in the cyber insurance market as a result of large ransomware payments has had a flown-on effect for quota-share reinsurance.

Globally, cyber reinsurance rates reportedly soared by up to 40 per cent in the financial 2020-21 financial year, attributed to a spike in ransomware attacks.[28] UK researchers have also highlighted the dynamism of cyber risk, stating "the insurance industry has likely never faced a risk that can change so drastically".[29] Hence, within the insurance and reinsurance industry, there are concerns a catastrophic cyber incident or sustained high-cost ransomware attacks could result in insolvency.[30] It has also resulted in increasing premiums and heightened requirements for coverage, putting it out of reach for many organisations, especially SMEs.

20. Does Your Cyber Insurance Cover a State-Sponsored Attack? (hbr.org)
21. Cyber Insurance: A Study In Fine Print (forbes.com)
22. Ibid 20
23. Ransomware, cybersecurity, and insurance | Secondary Sources | National | Westlaw Today
24. Ibid 23
25. ibid 18. P10
26. ODNI_A_Guide_to_Cyber_Attribution.pdf, P2
27. What is reinsurance? | CGU Insurance
28. Global Cyber Reinsurance Rates Soar by as Much as 40% During July Renewals: Willis Re (insurancejournal.com)
29. Cyber Insurance and the Cyber Security Challenge (rusi.org), P31
30. Ibid 29. PP32-33

PROBLEMS WITH CYBER INSURANCE

EXTORTION PAYMENTS

Many cyber insurance policies offer explicit coverage for extortion and ransom payments. This is problematic, serving to feed the criminal enterprise of ransomware gangs, especially those that prey on insured organisations.[31] There is evidence from overseas that ransomware criminals have accessed systems in search of insurance certificates and then demanded ransom payment of the specific amount covered by an insurer.[32] Furthermore, ransomware gangs have hinted at targeting insurers themselves, with a representative from notorious ransomware gang REvil telling a reporter the gang aims 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".[33]

Former head of the UK's National Cyber Security Centre, Ciaran Martin, recently voiced his concerns regarding the practice of insurers paying ransoms. He said: "You have to look seriously about changing the law on insurance and banning these payments, or at the very least, having a major consultation with the industry".[34] The OECD has also highlighted the practice as problematic, noting that cyber insurance may be "unintentionally facilitating the behaviour of cybercriminals by contributing to the growth of targeted ransomware operations".[35]

A review of 35 publicly available cyber insurance policies from countries including Australia, Canada, Japan, Netherlands, United Kingdom and the United States, was recently conducted by the OECD. Of the eight policies offered in Australia, all provided explicit coverage for ransom payments, with just three applying conditions for the coverage.[36]

While ransomware payment should not be criminalised, there is merit in moves to ban the payment of ransoms by insurance providers. While this may be an area where government regulatory intervention is required, individual insurers could choose to exclude these payments from insurance policies and provide greater focus on remediation and business continuity expenses. This is not without precedent. In May 2021, global insurance company AXA announced it would stop writing cyber insurance coverage in France that reimburses customers for making ransomware payments.[37] And at a recent hearing of the Australian Parliament's House of Representatives' Standing Committee on Economics, representatives from insurers IAG and QBE endorsed a review of the practice.[38] Adding further weight to the argument, the OECD observed that "a broad restriction on the reimbursement of ransom payments would allow (re)insurance companies to remove that coverage without being left at a competitive disadvantage".[39]

31. CSIAC, Locked out: tackling Australia's ransomware threat, 9.
32. Cyber Insurance Firm Suffers Sophisticated Ransomware Cyber Attack; Data Obtained May Help Hackers Better Target Firm's Customers - CPO Magazine
33. Does It Ever Make Sense for Firms to Pay Ransomware Criminals? (insurancejournal.com)
34. Insurers 'funding organised crime' by paying ransomware claims | Malware | The Guardian
35. Ibid 29. P36
36. Ibid 18. P20
37. Does It Ever Make Sense for Firms to Pay Ransomware Criminals? (insurancejournal.com)
38. IAG, QBE call for ban on cyber ransom payments (afr.com)
39. Ibid 18. P24

RANSOM BROKERS – WORKING IN THE SHADOWS

There is little publicly available information about ransomware brokers. These brokers are hired – sometimes by insurance companies – to negotiate ransom payments and pay ransoms in bitcoin. There is no regulation of such brokers and, concerningly, the legality of their role in the ransomware economy, and their very business model, is questionable.

In the US, where ransomware brokers operate more visibly, some have spoken about their trade. However, opaqueness reigns. For example, in an interview with Forbes, a negotiator and broker from Coveware would not "give much away about his negotiating tactics", while insisting the firm had ways to glean information about attackers to determine whether payment was in breach of US sanctioned entity laws.[40] In a separate interview, a broker from MonsterCloud said "we work in the shadows" and use dark web contacts to facilitate negotiation and payment.[41]

INSURER AS SHADOW DIRECTOR

In the event of a serious cyber incident, it is vital that senior management and boards have overview and insight into decisions that are being made. However, most cyber insurance policies include provision for the complete management of a cyber incident, right from technical incident response through to public relations and media. This is risky for organisations, with the role of insurer potentially extending into shadow directorship.

Under Section 9 of the Corporations Act 2001 (the Act) a person may be considered a director if:

- they act in the position of a director – referred to as a "de-facto director"; or
- the directors of the company are accustomed to act in accordance with the person's instructions or wishes – referred to as a "shadow director".[42]

In 2016, former ASIC Commissioner John Price highlighted the risks associated with shadow directorship, stating that: "Shareholders, creditors, employees and other stakeholders are entitled to know who makes, or participates in making decisions that affect the business, so that they can make fully informed decisions about their investment or relationship with the company".[43] When it comes to cyber insurance and the ability of insurers to effectively 'take over', this statement should sound alarm bells.

In the insurance industry, cyber insurers often refer to their role as "incident response manager" or "breach coach". They outsource incident response work to preferred vendors to carry out work ranging from network security and digital forensics through to ransom negotiation and payment. This could mean that insured organisations are unable to call in the services of their own lawyers, communications teams or even IT staff. In terms of reputational risk, such a scenario is rife.

Ultimately, the step-in powers insurers yield have the potential to equate to reputational risk. In the event of a serious cyber incident senior management and the board should remain in charge of risk and have oversight over all major decisions. There is a need for them to take a leading role in specific parts of incident reaction and response, in congruence with their duty to shareholders.

40. Meet The Firm That Pays Bitcoin Ransoms On Behalf Of Its Customers (forbes.com)
41. The Trade Secret: Firms That Promised High-Tech Ransomware Solutions Almost Always Just Pay the Hackers (propublica.org)
42. Jumping at shadows – shadow and de facto directors (sparke.com.au) P 49
43. Shadow directors in the spotlight - Australian Institute of Company Directors

COMPLACENCY

There is potential for organisations holding cyber insurance to be lax in their approach to managing cyber security. As noted in the Harvard Business Review: "Insurance is important, but it's likely to take a back seat to the broader cyber security discussion...Insurance helps you recover from a situation, filling in the gaps when problems occur that you can't prevent, but attempts to prevent problems are still crucial".[44] Some have also observed the 'moral hazard' associated with cyber insurance, with some organisations potentially less likely to invest in adequate cyber security if there is a belief cyber insurance policy will resolve an incident at less cost.[45]

Such a trend has been noted in New York, where the state insurance regulator, the Department of Financial Services (DFS), this year relayed a stern guidance. The DFS's Cyber Insurance Risk Framework, which was released on 4 February, states: "Insurers that don't effectively measure the risk of their insureds also risk insuring organisations that use cyber insurance as a substitute for improving cybersecurity and pass the cost of cyber incidents on to the insurer".[46] The DFS recommended that vigorous review of the cyber security maturity of policy holders or potential policy holders be completed, encapsulating corporate governance and controls, vulnerability management, access controls, encryption, endpoint monitoring, boundary defences, incident response planning and third-party security policies.[47] The DFS also highlighted the key role insurers can play in educating policy holders about the importance of cyber security and reward those practising good cyber security through lower premiums.

44. Cybersecurity Insurance Has a Big Problem (hbr.org)
45. Ibid 29. P37
46. Insurance Circular Letter No. 2 (2021): Cyber Insurance Risk Framework | Department of Financial Services (ny.gov)
47. Ibid 46

THE ROLE CYBER INSURANCE CAN PLAY IN BOLSTERING CYBER SECURITY

SETTING MINIMUM STANDARDS FOR COVERAGE

There is evidence cyber insurance policies vary significantly in terms of eligibility criteria, with some insurance questionnaires focussing more heavily on an organisation's cyber maturity than others.[48] Furthermore, there is little information available regarding the minimum cyber security measures an organisation should have in place to be eligible for cyber insurance. This is a missed opportunity. There is clear scope for cyber insurers to set minimum cyber security standards for coverage, encouraging cyber security uplift across the segment of the economy seeking to take out these policies. Such standards could be consistently set across insurance companies to help achieve greater harmony and clarity around cyber insurance policies. A standardised *Cyber Security Checklist* could be an effective tool to drive such action.

It is interesting to note that in the US, some insurers have begun to acknowledge the cyber security uplift they can help grow. For example, at one of President Biden's recent cyber security panels, the CEO of large insurer Vantage, Greg Hendrick, stated "the insurance industry can play a vital role by bringing a more risk-based approach to providing coverage and pricing of cyber insurance … we need to be prepared and mitigate what has yet to be seen; a true catastrophic scenario where an attack is able to impact thousands of companies".[49] Also, as noted previously, US insurers Resilience and Coalition have announced new measures they will implement to bolster cyber security, with Resilience setting baseline cyber security standards for coverage and Coalition making its cyber security assessment and monitoring platform freely available to any organisation.[50] According to Coalition, the platform is suitable for organisations of all sizes.[51]

Such an approach is prudent given the tightening cyber insurance environment. There is evidence insurers may not cover organisations that cannot adequately demonstrate effective cyber security protocols are in place.[52] It also offers a clear path to incentivisation of cyber insurance, with lower premiums for organisations that demonstrate cyber resilience.

A CYBER SECURITY CHECKLIST?

The introduction of a standardised *Cyber Security Best Practice Guidance Checklist* for insurers could help guide SMEs by setting out the minimum cyber security protocols they should have in place when seeking cyber insurance. It is important to note such a checklist would act as a best practice guide only, not ensuring cyber insurance coverage. It would, however, provide SMEs with greater clarity regarding the minimum level of cyber maturity they should aim to reach and have in place to be considered for a cyber insurance policy.

This best practice guide for SMEs should include:

- multi-factor authentication – used for access to all key systems
- patching program in place – with focus on patching vulnerabilities within the recommended timeframes
- antivirus software installed and regularly updated
- regular data backups conducted, including onsite and offsite storage
- password policy in place and implemented by all staff
- annual cyber security training for staff
- clear policies around internet access; remote access; use of personal and portable storage devices (such as USBs); work email and communications in place
- access management across all systems so only the right amount of staff have access to information in order to do their job

48. Ibid 5
49. "Vital role" of re/insurance stressed at White House cyber meetings - Reinsurance News
50. Ibid 10
51. Introducing free attack surface monitoring with Coalition Control | Coalition (coalitioninc.com)
52. Ibid 12. P4

BUNDLING SERVICES

Insurers can play a role in the bundling of cyber security tools to help uplift the cyber security of their client base. There is scope for insurers to partner with telecommunications providers, cloud services and software providers to provide the tools necessary for cyber security uplift as part of a 'bundled package' comprising insurance and cyber security products. As noted above, US insurance firms Resilience and Coalition are taking steps towards this type of incentivisation. Another good example of this type of approach is that of Amazon in the US, which announced it would freely provide a multi-factor authentication device to Amazon Web Services account holders.[53]

Importantly, such a move would align with the objectives of *Australia's Cyber Security Strategy 2020*, with regard to SME cyber security uplift. The strategy states: "The Australian Government will work with large businesses and service providers to provide SMEs with cyber security information and tools as part of 'bundles' of secure services (such as threat blocking, antivirus, and cyber security awareness training). Integrating cyber security products into other service offerings will help protect SMEs at scale and recognises that many businesses cannot employ dedicated cyber security staff".[54]

ENCOURAGE INCREASED AND TIMELY REPORTING OF DATA BREACHES

Cyber insurance has the potential to help drive regulatory compliance in relation to notifiable data breaches. Increased and more timely reporting could be achieved because insurers could refuse to pay claims if regulatory requirements were not met by an affected organisation.

The Privacy Act 1988 (the Act) is the key legislative tool to protect the privacy of individuals and regulate how Australian Government agencies and organisations with an annual turnover of more than $3 million, handle personal information. In 2018, changes to the Act came into effect, amending it to include the Notifiable Data Breaches (NDB) scheme. The scheme applies to any organisation or agency covered by the Act.

If an organisation suspects an eligible data breach has occurred, they must undertake an assessment into the relevant circumstances. And if an entity is aware there are reasonable grounds to believe there has been an eligible data breach and risk of serious harm, they must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) as soon as practicable[56].

However, there is evidence such regulatory requirements are being shirked by some organisations. In the OAIC's *Notifiable Data Breaches Report – January to June 2021*,[57] issues regarding NDBs and ransomware attacks were highlighted. According to the OAIC, "a number of entities assessed that a ransomware attack did not constitute an eligible data breach due to a 'lack of evidence' that access to or exfiltration of data had occurred".[58] Such behaviour was called out by the OAIC as being out of line with the regulatory requirements of the NDB scheme, warning that "it is insufficient for an entity to rely on the absence of evidence of access to or exfiltration of data to conclusively determine that an eligible data breach has not occurred". Given what is known about the modus operandi of ransomware criminals, data is exfiltrated during an attack to be applied later as a bargaining chip.[59] The assertion that the 'absence' of evidence of data theft does not mean data has not been stolen and, if used as a means to avoid reporting to the OAIC, is a worrying trend. Hence, any moves to ensure increased and timely reporting of data breaches would be beneficial.

53. Ibid 10
54. Australia's Cyber Security Strategy 2020 (homeaffairs.gov.au), P8
55. About the Notifiable Data Breaches scheme – OAIC
56. When to report a data breach – OAIC
57. Notifiable Data Breaches Report (oaic.gov.au)
58. Ibid 57. P18
59. Exfiltrate, encrypt, extort | Australian Strategic Policy Institute | ASPI

CONCLUSION

Cyber insurance is vexed and highly nuanced. While it can support cyber security uplift, it can also have the opposite effect, breeding complacency and feeding the cyber-crime economy.

Given the market is still young in Australia, the time is ripe to ensure cyber insurance is a help, not a hindrance, because there is a positive role it can play. And central to achieving this is regulation and transparency. There is a clear role for insurers to include minimum cyber security best practice guidance as a precursor to any policy being taken out and, furthermore, greater clarity is needed in relation to what is and what is not covered and the circumstances under which a claim may be refused.

Most importantly, cyber insurance should not be seen as an organisational cyber security strategy – a panacea to any incidents that may occur. Nor should insurers be permitted to pay extortion payments, a trend which has not only fuelled the ransomware trade, but also placed extraordinary pressure on the viability of the cyber insurance industry itself.

RECOMMENDATIONS

Australian insurers offering cyber insurance policies should be prohibited from making any ransom or extortion payments as part of any cyber insurance offering – the focus should be on response and recovery.

APRA, like the prudential regulator in the UK, should provide a guidance outlining its expectations regarding the management of cyber insurance underwriting risk. Such guidance should also require insurers to clearly articulate what is and is not covered, and where exclusions may apply.

Insurers should work together to develop a *Cyber Security Best Practice Guidance Checklist* for SMEs, setting out the minimum cyber security settings and policies they should have in place when seeking cyber insurance. This could help improve SME cyber security and reduce risk for insurers.

Insurers should work with telecommunications providers, cloud services and software providers to provide 'bundled packages'. Such partnerships could be incentivised by the Federal Government, which could support pilots of such packages.

Australian Government
Department of Industry, Innovation and Science

Business
Cooperative Research Centres Program

THE CYBER SECURITY COOPERATIVE RESEARCH CENTRE

cybersecuritycrc.org.au