Insurance Council of Australia

Cyber Insurance: Protecting our way of life, in a digital world

March 2022

insurancecouncil.com.au

Contents

Cyber Insurance: Protecting our way of life, in a digital world

A discussion paper about the implications of cyber incidents on Australian businesses and recommendations for a sustainable cyber insurance market.

Introduction

The last decade has witnessed unprecedented growth in digitisation and connectivity between individuals, businesses, and governments around the world. This has had a profound impact on the way all businesses, from small family-based enterprises to multinational conglomerates, conduct their operations.

The digital evolution of both the economy and society has brought with it efficiencies, opportunities and an adaptiveness that made Australia resilient during the upheaval of the COVID-19 pandemic. However, this interconnectedness has also been accompanied by significant, and increasing, cyber risks arising from both domestic and overseas sources.

Cyber risk primarily refers to the risk posed to a business by a data breach or network compromise. These can occur as a result of either human error, malicious actions by disgruntled employees, by organised crime gangs, acts of war or disruption by nation states. Insurance is an important component in managing this rapidly growing threat to business viability as it can provide risk mitigation and risk transfer. Cyber insurance as a product has evolved to support businesses to manage these risks.

Across the cyber risk spectrum, the nature of cyber risk at the extreme end has evolved, and increasingly criminal gangs and nation states are targeting business operating systems. This act directly attacks a businesses' ability to function, retain data securely, access important data and make money. The challenge posed by extreme, sophisticated, and well-resourced threat actors will lead to further evolution in cyber insurance.

Right now, cyber insurance awareness is low within the Australian business community and there is a small number of insurance providers. The combination of a small premium pool and the increasing sophistication and maliciousness of some cyber-attacks have put significant pressure on insurers and businesses alike. Many insurers are reluctant to provide cyber insurance, or instead provide limited insurance cover, given the high cost and difficulty in pricing cyber risk due to its rapidly changing profile. If appropriate insurance is not available for businesses to mitigate cyber risk, many may not be able to, or may be reluctant to, adopt more innovative practises. This will hinder Australia's economic productivity.

Our accelerated digital economy and interconnectedness is not going away. By extension, the demand for cyber insurance products that are readily available, affordable, and sustainable will only grow. While cyber risk is a global and national issue, it is important for the government and industry to work together to ensure policy settings and collaborative data sharing to support a vibrant and sustainable domestic market to meet that demand. There are also a number of risk mitigation strategies which can be undertaken at the individual and business level to significantly reduce cyber risk and support an Australian cyber insurance market. Getting the settings right for the management of cyber risk will give insurers greater confidence in participating in the market and providing cover.

A viable cyber insurance market will support the resilience of the Australian economy and the prosperity of businesses small and large.

Cyber insurance trends

Overview of the market

Cyber insurance arose as a distinct product in California in the 1990s. It is now a global insurance product, and it is becoming an increasingly specialised product, as insured businesses have become further digitised. This stand-alone product offering helps policy holders to respond to cyber incidents and manage any associated business interruption by providing financial support and access to expert support services through the recovery process. Globally, it is estimated that written premiums total around USD $4-5 billion, increasing from USD $3 billion in 2016.[1] This is expected to potentially "double or triple over the next five years".[2]

Whilst the cyber insurance market continues to grow, internationally and in Australia, the take-up rates remain low compared to more traditional commercial property and liability insurances.[3] At the same time, cyber-related losses continue to rise in both frequency and severity. Insurers continually monitor and adjust their risk appetite and capacity, together with coverage, limits, and pricing, both in Australia and globally.

Figure 1: H1 Australian cyber market snapshot

Source: Marsh, Mid-Year Insurance Market Update 2021, 8

In recent years, the number of organisations taking up cyber insurance in Australia has been increasing. Marsh[4] found that in the first half of 2021, there was a 23 per cent increase in the uptake of cyber insurance in Australia, attributing that increase to a heightened level of awareness around cyber risks. While there has been an increase in the uptake of this form of insurance, so has there been an increase in the loss ratios for the product.[5] This has led in some cases to insurers withdrawing from the market, limiting capacity, or introducing co-insurance requirements, making cyber insurance difficult to obtain in some circumstances.

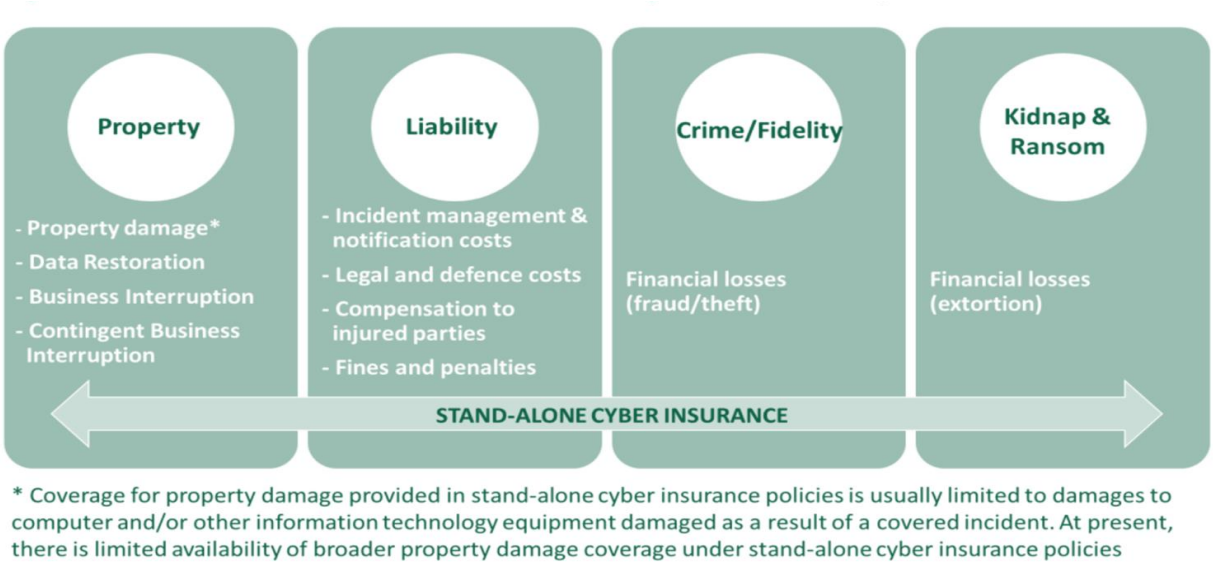
1 OECD, *The Role of Public Policy and Regulation in Encouraging Clarity in Cyber Insurance Coverage*, 2020, 5
2 Ibid
3 OECD, Insurance Coverage for Cyber Terrorism in Australia, February 2020, 13
4 Marsh, Mid-Year Insurance Market Update 2021, 8
5 Ibid

A particular trend which is challenging insurers is an increase in ransomware claims. Marsh found that in Australia, in the first quarter of 2020, “premium increased by 20-30%, and in the second quarter, by 60-80%, compared to the same periods from last year, respectively”.[6] They attributed this to increased claims activity and noted that this was consistent with global trends.

However, we understand from members that any actual payment of ransom by the victim business comprises a small proportion of most claims.[7] Instead, considerable funds are expended looking at what the hackers did when they were inside the compromised system (for example, what data sets etc they were interested in, what action they took). Given this, forensic analysis, and business interruption costs are where the costs primarily lie.

Cyber coverage

Figure 2: Losses & cost covered under cyber insurance



Source: The International Association of Insurance Supervisors (IAIS) Cyber Risk Underwriting December 2020

In Australia, general insurers provide stand-alone cyber insurance policies to businesses to cover a range of losses related to cyber incidents. Coverage is typically available for:

- costs related to the loss of or damage to data;
- content-related claims related to data;
- investigation and remediation costs;
- public relations costs;
- liability for denial of service from or access to electronically provided data;
- costs association with cyber extortion reimbursement;
- fines and penalties imposed by regulators; and
- compensation to third parties for failure to protect their data.

6 Ibid

7 Allianz, *Cyber insights 2021, Ransomware trends: Risks and Resilience*

Of the coverage types listed above, the first six are ‘first-party’ as they cover losses incurred directly by the insured, while fines and penalties; and compensation are both ‘third-party’ as they cover losses incurred by third parties (in the case of fines, the third party is the relevant regulator) that may subsequently be recouped against the insured. The nature and limits of cover will vary by insurer. Property losses relating to damage or corruption of data are typically excluded.

In the case of cyber, the Office of the Australian Information Commissioner (OAIC) is the privacy commissioner who commences the investigation/prosecution which may lead to fines and penalties being levied. As a matter of policy, fines and penalties are a legitimate tool in driving changes of behaviour within a particular market. However, they need to be used judiciously to avoid giving rise to unintended consequences. In the context of the cyber insurance market experiencing a rapid rise in loss ratios, a less than targeted use of this tool, including legal action, may inadvertently contribute to emerging affordability issues across the broader market.

Cover for cyber exposure may also be available as an additional element of business insurance packages, such as management liability and professional indemnity. In this case, the insured business purchases the primary cover, and elects to include some cyber-specific cover for additional premium. This form of cover is more limited than stand-alone cover.

Discussion points

Silent cyber

Historically some non-cyber policies may have included some cover for cyber incidents captured under the existing terms of the policy, where they are not specifically excluded. This is referred to as 'silent cyber' or 'non-affirmative.' Examples of cyber incidents involving silent cyber losses were the 2017 NotPetya and WannaCry global malware attacks, which led to claims under property policies. These attacks, deployed through computers operating Microsoft Windows, had a devastating impact on the operations of many organisations. The WannaCry ransomware crypto-worm was estimated to have infected more than 230,000 computers across at least 150 countries.[8] Generally, under standalone cyber insurance, these claims would have explicit coverage under the policy. That said, not all silent cyber claims will be covered under a cyber policy. Those claims that arise from social engineering fraud, such as phishing, may not be covered. There will also potentially be gaps in cover between a cyber policy and a non-cyber policy with a cyber exclusion.

Insured losses from these two attacks were extensive, in part because of the broad nature of the original security and privacy insurance policy language for first-party coverages, such as system failure and business interruption. The NotPetya attack is estimated to have had an economic cost of US$10 billion.[9] The widespread damage that these attacks caused underlines how extensive first-party coverage components can be. The global magnitude of the damage from WannaCry and Petya/NotPetya also demonstrates the speed at which cyber-attacks spread and the risk of proliferation and accumulation.

The reinsurance market has tightened silent cyber conditions in recent years and as a result, property policies are now more likely to explicitly include, or exclude, cyber cover. Regulators are also influencing insurers and reinsurers to measure and monitor their cyber exposures and be explicit as to coverage under general business and standalone cyber insurance products.[10]

Recommendation

The insurance industry works with policyholders to ensure that they clearly understand the extent to which (if at all) cyber risks are covered in their non-cyber insurance policies.

Insurers in the Australian market to work with reinsurers to understand what they require to enable adequate coverage of risks within cyber policies sought. These requirements can then be addressed at an industry level by working collaboratively with stakeholders to increase capacity within the cyber insurance pool.

8 Oxera, The value of cyber insurance to the UK economy, 2

9 Ibid.

10 Bank of England, Prudential Regulatory Authority, *30 January 2019 Letter to Chief Executives of specialist general insurance firms regulated by the PRA*

Acts of war coverage

The increasing sophistication and frequency of nation state cyber-attacks also has implications for war coverage. State-sponsored cyber-attacks that stop short of outright military conflict pose a particular challenge for insurers. Traditional policy exclusions for war or war-like incidents might fail to capture situations where nation states are suspected of being behind an attack, or providing a safe harbour for the hackers, especially if the motives for the attack are unclear. Such issues of attribution and characterisation create significant contractual uncertainty for insurers, which has only added to the recent tightening in cyber insurance market conditions.

This was demonstrated in the January 13, 2022, New Jersey Superior Court's decision in favour of Merck and International Indemnity. In this case, the Court sided with Merck's stance that its insurers cannot assert the property policies' war exclusion to avoid coverage of losses from the 2017 Notpetya malware attack. The parties disputed whether the Notpetya malware, which affected Merck's computers in 2017, was an instrument of the Russian government, so that the War or Hostile Acts exclusion would apply to the $1.4 billion loss. The Judge found that war exclusion precludes only a physical act of warfare and not a malware hack unless otherwise specified by insurers in the policy.[11]

Quantifying risks from state sponsored incidents is extremely difficult. It could range from minor isolated incidents to full-out cyber warfare. The size of potential losses from a major cyber incident relative to the extent of cover currently provided by insurers, highlights a significant protection gap. Given this, insurers have tightened conditions for affirmative and non-affirmative cyber insurance by maintaining modest limits on individual affirmative cyber policies and, increasingly, explicit exclusions on non-affirmative contracts to eliminate silent cyber. For example, Lloyds of London have developed model exclusion clauses for standalone cyber insurance policies to ensure cyber war and cyber operations are excluded.[12]

The Geneva Association and International Forum of Terrorism Risk (re)Insurance Pools research recommends that a government backed solution or public-private partnership is needed to meet extreme cyber risks to boost economic resilience.[13]

Recommendation

The Government should continue to monitor and consider the merits of expanding the current Terrorism Risk Insurance Pool to include extreme cyber incidents to ensure the viability of a private market for cyber insurance and boost economic resilience.[14]

The industry should consider encouraging insurers to review their current policy wording regarding acts of war and if needed, consider developing model wording to ensure cyber incidents are excluded where intended as part of the acts of war exclusion.

11 https://news.bloomberglaw.com/privacy-and-data-security/mercks-1-4-billion-insurance-win-splits-cyber-from-act-of-war

12 Lloyd's Market Association, *Bulletin LMA21-042-PD Cyber War and Cyber Operation Exclusion Clauses 25 November 2021*

13 The Geneva Association and International Forum of Terrorism Risk Insurance Pool, *Insuring Hostile Cyber Activity: In search of sustainable solutions January 2022*

14 Noting Treasury's view that the scope of the ARPC should not be extended at this time to cover this risk, Terrorism Insurance Act Review, December 2021 at 11.

Data analysis

It is recognised that there are significant difficulties in using data to predict risk for cyber insurance. This is because:

- Cyber-crime is rapidly increasing and evolving, making historical data of limited use for predicting risk accurately.
- Current data collected by Government agencies may not be complete or subject to some level of reporting discretion by the regulated firm, or may not be available to insurance companies.
- Requirements may only apply to certain industry sectors and therefore does not provide economy wide data.

For example, here in Australia, the Australian Cyber Security Centre (ACSC) collects reported cyber-attacks from individuals and entities through ReportCyber. For the 12 months ending 30 June 2021, the ACSC reported that there had been 67,500 reported cyber-attacks (an increase of 13% on the prior year) with self-reported losses from cybercrime totalling A$33 billion. Medium sized businesses had the highest average financial loss per cybercrime reported (A$33,442) as compared to A$19,306 for large organisations and A$8,899 for small businesses. Commonwealth, state, territory and local government accounted for 35% of the reports filed, which the ACSC acknowledges is in part due to the obligation of those organisations to report significant cyber security incidents to the ACSC. However, given the ACSC relies on self-reporting and focuses on government entities, it is unlikely that this provides a complete picture of the cyberattacks experienced across Australia.

Alternatively, the Office of the Australian Information Commissioner (OAIC) requires mandatory reporting of data breaches if the disclosure of personally identifiable information is likely to result in serious harm under the Privacy Act 1988;[15] and the Australian Prudential Regulation Authority (APRA) requires notifications of Information Security Incidents and Material Information Security Control Weaknesses under Prudential Standard CPS 234 Information Security (CPS 234).

While this data is collected by federal agencies OAIC and APRA, it does not address the data needs of insurers. The APRA data is not available publicly or to insurers. Further, both the OAIC and APRA breach reporting rely on subjective judgement regarding materiality and specific criteria, so does not provide the “full picture” of the number and nature of cyber-attacks which is needed by insurers.

The incentives to report need to be examined also in the context of enforcement or application of fines. However, complete information may be difficult to achieve when victims of cyber-attacks face disincentives to provide full reports, such as fines. There are also likely to be reputational issues which could incentivise firms to “under report” breaches. This could occur by establishing high bars for breaches to meet required criteria or to be classed as serious under the Privacy Act 1988.

Further, timely reporting data also provides an opportunity for risk mitigation, as well as good policy settings. Thought needs to be given as to how information on attacks can be disseminated in a real-time manner, while protecting victim confidentiality, to help prevent further Australian businesses becoming victims.

15 https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics

Recommendation

Further work is required to increase the sharing of data around cyber incidents, both from industry to government and from government to industry. There is also a need for increased understanding of cyber risk in the business community to prevent, detect and report on cyber incidents. The reporting and sharing of this data would significantly contribute to the ability to identify, understand, and control the cyber risks and ensure that insurance was properly designed to mitigate losses from these risks A key challenge will be addressing privacy and commercial confidentiality requirements.

Software and hardware industry

Cyber-attacks can be reduced by ensuring the software and hardware used in networks does not contain vulnerabilities. Recently there has been significant exploitation of weaknesses in the design of software and hardware used by government and industry to facilitate cyber-attacks. For example, the discovery of malware in the file of NPM's JavaScript library packages, which are used by the likes of Facebook, Microsoft, and Amazon. One such instance in 2021 was where an attacker modified the library so they could install a password stealer and cryptocurrency miner on computers and servers.[16] However, at present, software and hardware products are not required in Australia to meet any minimum cyber security requirements to protect against cyberattacks.

Implementing minimum product design standards to reduce the opportunity for a cyberattack could be one effective risk mitigant for cyber insurance. Recognition of minimum standards through certification could standardise and provide certainty to product users upon purchase. Many governments have begun to consider and implement minimum standards to improve cyber resilience.

- On 13 July 2021, the Australian Government, Department of Home Affairs consulted on options for regulatory reforms and voluntary incentives to strengthen the cyber security of Australia's digital economy, which included minimum standards for hardware and software.[17] This process is ongoing, and a final report has not yet been released.
- The US Government began developing a variety of initiatives related to the security and integrity of the software supply chain to enhance cybersecurity in response to the May 2012 executive order, "Improving the Nation's Cybersecurity (14028)". Initiatives include developing guidelines recommending minimum standards for vendors' testing of their software source code, and two labelling programs related to the Internet of Things (IoT) and software to inform consumers about the security of their products.
- The UK plans to introduce legislation requiring hardware, such as smartphones, to provide security support and software updates during the life of the product.[18] The law will require devices to have unique passwords, to operate a vulnerability disclosure program, and inform consumers on the length of time products will be supported. Initiatives such as these should be considered for the Australian context.
- Cyber Security Agency of Singapore (CSA) introduced several initiatives to improve IoT security. This includes introducing a cybersecurity labelling scheme in October 2020.[19]

---

16 ITWorld Canada, *Cyber Security Today, Oct. 25, 2021 – A warning to JavaScript users, ransomware gangs feeling squeezed and an SQL vulnerability found*

17 Australian Government, Department of Home Affairs, *13 July 2021 Discussion paper Strengthening Australia's cyber security regulations and incentives*

18 UK Government, Department for Digital, Culture, Media & Sport 1 December 2021, *Guidance: The Product Security and Telecommunications Infrastructure (PSTI) Bill - product security factsheet*

19 Cyber Security Agency of Singapore, *Press release 6 October 2021 CSA Pushes Ahead with Efforts to Improve IOT Security*

Recommendation

Working with industry, the Government should continue to develop minimum security requirements and third-party certifications for software and hardware to reduce the vulnerability of software and hardware to cyberattacks as per its commitment as part of Australia's Cyber Security Strategy 2020.[20]

Accumulation

A major cyber event or a smaller series of connected successive attacks could render cyber insurance financially unviable. The impact of an accumulation event is of underlying concern to many insurers. For example, WannaCry and Petya/NotPetya demonstrated the velocity and scale at which cyberattacks spread on a global scale and the risk of accumulation.

Unlike for other events such as cyclones or floods, catastrophe modelling by government and industry to estimate the losses that could be sustained due to a catastrophic cyber event in Australia is not well developed. Sophisticated modelling requires high quality data. As cyber insurance in relation to extreme cyberattacks are still in its relative infancy, greater efforts need to be made across government and industry to collaborate and collate data for better understanding, analysis, and modelling. For example, the Singapore Government has invested in the Cyber Risk Management (CyRiM) project led by NTU-IRFRC in collaboration with industry partners and academic experts. CyRiM is a pre-competitive research project that aims to foster efficient cyber risk insurance. Part of this project involved creation of cyber loss models and cyber event scenarios for impact quantification and study of accumulation risk in systemic events.[21]

Critically, without enhanced cyber catastrophe risk modelling insurers could underestimate exposures to major cyberattacks. This could have substantial negative financial impacts on insurers with subsequent adverse impacts across the economy.

Recommendation

Industry to collaborate with Government and relevant agencies to facilitate and create incentives for the development of cyber risk modelling.

Ransomware

Ransomware sits at the extreme end of the cyber risk spectrum. However, it continues to grow as a cyber security threat, with the insurance industry developing standalone cyber products and associated expertise to help prevent and manage attacks.

The cyber insurance market has evolved to cover ransomware, which includes not just indemnification of ransoms paid but also the other related loss events. In many cases, the ransom payment, if it is paid by the victim, may only be a minor part of the total loss that could be covered by insurers. However, it has attracted comment, and has the potential to hinder a measured policy response which supports the economy.

---

20 Australian Government 2020, Australia's cyber security strategy 2020

21 The Cyber Risk Management Project accessed 27 January 2022

The insurance industry recognises that the payment of cyber ransoms, and proposals to ban ransom payments in law, are vexed public policy issues. Theoretically reimbursing ransoms under insurance policies could increase moral hazard and provide an incentive for increased cyberattacks and reduced protections against cyber-attack.

However, this does not appear to be the case for cyber insurance and the arguments put forward for banning indemnification under policies are weak. For example, it is suggested that the existence of a policy indemnification encourages criminals to commit the cybercrime, therefor if that indemnity were prohibited the crime would not occur. More logically, if the indemnity were prohibited the criminal would simply use another metric to quantify the ransom demand. For example, the amount of cash the business has in in the bank, or on term deposit, or the maximum overdraft that can be drawn down under its banking arrangements, the amount of any guarantee specified under an owner guarantee, etc. There are numerous other metrics the cyber-criminal could use to quantify the ransom demand.

There are also much more significant incentives present for businesses to protect themselves and pay ransoms. These include the cost of business shutdowns, reputation and lost sales. For example, although Colonial Pipeline had backups, the need to restore services swiftly pushed them to pay the ransom.[22] The iRansomware victims included small and medium businesses who did not necessarily have the capability and systems to effectively protect themselves from attack. By banning such payments, regulators may be removing one of the mechanisms a business would have to save itself and protect its customers. Directors and executives of small and medium businesses have few options and little support in these circumstances. Moreover, the net effect would be to victimise the innocent business twice; first by the cybercriminal and then by the policy decision to prevent it from insuring against that particular risk.

The Australian Government recently released a Ransomware Action Plan, which formally identifies that the Government does not condone ransom payments. This position is consistent with that of other governments around the world, which have thus far discouraged the payment of ransoms but not chosen to ban the victims of ransomware attacks from making such payments. Instead looking at mandatory reporting, increasing capability and providing direct assistance as measured policy approaches to reduce the incidence of ransomware attacks. Additionally, on 2 December 2021 the *Security Legislation Amendment (Critical Infrastructure) Act 2021* amended the *Security of Critical Infrastructure Act 2018* (SOCI Act) to include mandatory reporting (including ransom demand) across eleven sectors, including: communications, financial services and markets, data storage or processing, defence industry, higher education and research, energy, food and grocery, health care and medica, space technology, transport, and water and sewerage.[23]

Further, international governments have called for nation states to take action against cyber-attacks originating in their jurisdiction. At the G7 Summit in June 2021, a joint statement of G7 countries called on Russia to do more to stop cyber-attacks and to “identify, disrupt, and hold to account those within its borders who conduct ransomware attacks, abuse virtual currency to launder ransoms, and other cyber-crimes".[24]

Recommendation

The Government to incentivise cyber victims to disclose ransomware events and seek affirmative assistance from law enforcement and reduce disincentives, such as punitive measures, which discourage disclosure.

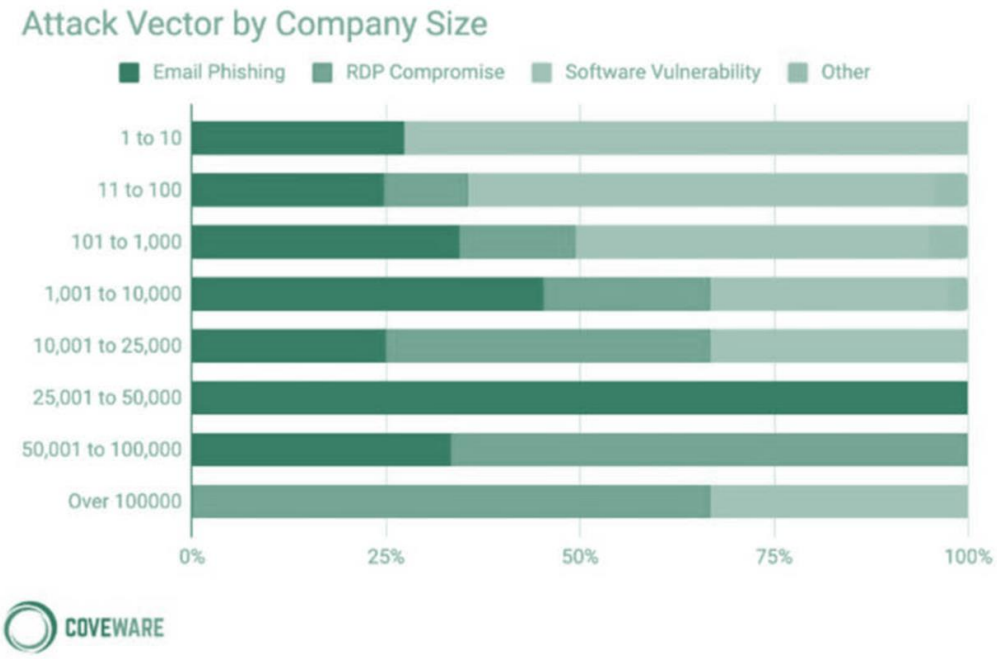
---

22 Royal United Services Institute for Defence and Security Studies (RUSI), Occasional Paper: Cyber Insurance and the Cyber Security Challenge, 28 June 2021

23 Amendments to the Security of Critical Infrastructure Act 2018, accessed 27 January 2022

24 The White House, *Carbis Bay G7 Summit Communique*, 13 June 2021

Figure 3: Attack Vector by Company Size



Source: New York State Department of Financial Services

According to New York State Department of Financial Services, the top industry classes impacted by ransomware claims in 2020: Government; Healthcare; Manufacturing; and Educational Services.

Case study: Cyber-attack on a pharmacy

The hypothetical case study demonstrates how cyber insurance works to help businesses and the types of costs that can be incurred in a cyberattack. In this incident, an independent pharmacist is subject to a ransomware attack that encrypts the data affecting their point of sales registers, rendering them unable to trade. Beyond the inability to trade, the pharmacist's systems contain sensitive health information regarding its customers that may now be compromised as the threat actor encrypts the data and attempts to exfiltrate that data to hold as ransom. The loss events incurred by the pharmacist now include lost sales, potential investigations and prosecutions that may follow the event, as well as any third-party claims by impacted customers.

As a first point of call, the forensic experts would need to be brought in to determine the cause and the scope of the breach, with the costs covered by the insurance provider. There would also be the costs around notifying the government regulator and impacted customers, which needs to occur within a small window of time and can involve a lot of manual work. This work can be quite expensive as it can require many individuals reviewing every piece of record that had been compromised to determine the information that had been compromised. Those costs are covered under a cyber policy.

During the period that the systems are down, the pharmacist may need to bring on contractors, or have staff work overtime to handle the business disruption.

Depending on the size of the business involved and number of customers, the insured may also need to incur costs to operate a call centre to manage inquiries from impacted individuals. For the pharmacist, they would need to engage a third party to operate a call centre for a period, which would involve establishing a script and standard questions and answers to deal with the expected influx of calls from concerned customers. Even where a company has its own call centre, they may need to bring in additional staff or cover overtime costs to handle the significant increase in calls dealing with the security breach. In addition, the pharmacist may need to bring in a public relations consultant to mitigate the reputational damage to the business as a result of the breach.

As part of its response to the breach of customer data, the pharmacist may need to provide monitoring services to impacted individuals, allowing the monitoring services to collect the compromised data and examine any fraudulent activity based on the information that had been compromised.

The pharmacist will also need to determine whether to pay the ransom demanded to obtain the key to restore the data and devices and return the customer data. This can include legal costs to determine the legality of paying such a ransom.

As we move into the recovery phase of the cyber claim, the pharmacist will need to have the electronic data restored and have IT experts engaged to remove any malware. At this stage, the pharmacist may also now need to establish a process to ascertain eligibility, quantify and pay any compensation due to customers or other third parties arising from the breach of customer personal information, as well as respond to and pay any regulatory fines brought against the pharmacist arising from the breach.

In Australia, companies and government agencies that lose sensitive personal data are required to notify affected individuals or face fines of up to A$2.1 million. Fines for serious breaches are likely to increase to 10% of a company's turnover to a maximum of $10 million if the draft Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 is passed.[25]

A real example of the impact of a cyberattack in the health industry occurred on 14 May 2021 in the Republic of Ireland.

[25] OAIC, *Higher penalties to help protect Australians' privacy*, Media Release 25 October 2021,

Case study: Cyber-attack on a health service

On 14 May 2021, the Health Service Executive (HSE) of Ireland suffered a major ransomware cyber-attack that caused all its IT systems nationwide to be shut down to protect the systems from further attack. As a result of the shutdown, hospitals could not access electronic records and had to rely on paper records, with many appointments cancelled, particularly those waiting for complex tests.

The HSE example is quite a severe, but a real example. It is also worth noting that of the systems which were shut down on 14 May 2021 in the Republic of Ireland, only 70% of these computer devices were back in use over a month later. It took another four months until September 2021 before it was reported that 95% of all servers and devices had been restored.[26] Therefore, the recovery time back to full operational efficiency can be quite extended.

Further, the HSE may well face fines as a result of any data breach from the cyberattack. In Europe, the European Union's *General Data Protection Regulation* (GDPR) can issue fines of up to EUR 20 million or 4% of the company's annual worldwide turnover of the preceding financial year, whichever is greater.

Recommendation

Create investment incentives for companies and governments to educate the population regarding cyber risk to ensure greater mitigation in all areas. In addition, positive incentives for businesses to disclose and work with enforcement agencies are needed to increase cooperation.

[26] HSE cyber-attack: Irish health service still recovering months after hack - BBC News

Risk assessment and standards

Insurers need to, and do, take steps to assess the risk being underwritten in a cyber insurance policy. This process involves assessing the likelihood of an attack on any company, which requires access to reliable cyber incident data, and the likelihood that such an attack would impact the policyholder. To do this, insurers need to make an assessment of any risk mitigants, such as, the company's cyber security controls to price the risk they would assume in writing the policy. However, the process also has wider economic benefits for the affected business.

Understanding the risk

Insurance underwriters place a strong focus on a customer's risk management and security culture when reviewing, assessing, and pricing the risk. Effective risk management, including a strong internal security culture, can be the most effective defence against threats. Capabilities that indicate a strong risk management and security culture may, for instance, include internal data handling and internet usage policies for all employees across the business, training of all employees on identifying and responding to a potential phishing attack, adequate prevention, detection, and response security capabilities and plans.

The current industry approach to assessing a customer's risk exposure is founded on, but not limited to, questionnaires developed by each insurer. These focus on entity level controls and specific prevent and detect controls. Entity level controls could include the existence of an appointed Chief Information Security Officer (CISO), adoption of a control framework such as ISO 27001. Specific prevent and detect controls could include daily backups that are encrypted and testing of those backups, multi-factor authentication and whether the company uses network security monitoring software and performs penetration tests on its systems.

More recently, industry has started to enhance the rigour of the underwriting process through the use of third-party telemetry and analytics to validate some responses in the questionnaire and provide a better assessment as to the risk of attack for an entity. These analytics might provide insights into the external internet traffic going through or related to an organisation, the level of patching being performed by the entity, and whether they have been exposed to unsecure websites. For example, underwriters will sometimes share this data with the policyholder as a way of raising security awareness and also to filter out any flaws in the data collected.

Globally, companies may adopt and obtain certification of their information security management system (USMS) in accordance with one of a variety of control frameworks, including ISO 27001, the US National Institute of Standards and Technology (NIST) Cybersecurity Framework, and SOC 2.

In Australia, ASIC currently uses the NIST Cybersecurity Framework to assess the cyber resilience of financial markets firms, which recognises the value of the NIST Cybersecurity Framework as an industry benchmark.[27] The NIST Cybersecurity Framework (the Framework) was created through collaboration between industry and the US government to promote the protection of critical infrastructure.[28] The Framework is voluntary guidance, based on existing standards, guidelines, and practices for organisations to better manage and reduce cybersecurity risk. In addition to helping organisations manage and reduce risks. It was designed to foster risk and cybersecurity management communications amongst both internal and external organisational stakeholders.

Other jurisdictions have also introduced additional frameworks and certifications such as the UK Government's Cyber Essential scheme, while Australia has the Information Security Manual (ISM), the "Essential 8" and Australia Small Business guide. Government, industry, and business would greatly benefit from increased coordination and alignment of these various frameworks to ensure consistency while also acknowledging business maturity and local considerations. This is similar to the approach adopted in the development of international accounting standards, which are developed by the International Accounting Standards Board and then adopted locally by various countries, after implementing certain local considerations where appropriate.

Recommendations

Firstly, the Government to develop and issue a single cybersecurity framework (similar to NIST) and secondly, ensure that government agencies and contractors with whom they do business evaluate their cyber maturity according to uniform and constantly evolving standards. This approach will help drive best practice cyber security practice across the Australian economy.

Minimum industry underwriting standards

The cyber insurance industry is, theoretically, well placed to help lift cyber security practises amongst clients who choose to purchase cyber security insurance, as opposed to self-insure. This view is predicated on the assumption that insurance providers are financially motivated to reduce claims and losses. This means that, in theory, there should be a 'push factor' from the insurance industry to raise standards and drive best practises. For example, the industry is well placed to drive the adoption of reputable cyber security standards or frameworks like Cyber Essentials, ISO27001 or NIST. This can happen in two ways: by requiring a potential purchaser of cyber insurance to be certified to a set of standards, or by drafting questionnaires that use them as a framework. Insurers could reward "better standards" with greater cover and/or lower premiums providing an incentive for organisations to improve standards.[29]

However, recent UK research also suggests that, to date, this has tended to be more or a theoretical possibility and that there are a number of practical impediments to insurance being used to lift cyber security practises in the business community.[30] Nonetheless, there are things which can be done that will help. Adopting standards at an industry level will address some of the challenges facing the development of cyber insurance standards on an individual business basis. These include:

---

27 ASIC 6 December 2021, *REP 716 Cyber resilience of firms in Australia's financial markets: 2020-21*

28 The National Institute of Standards and Technology (NIST) December 2021, Cybersecurity Framework

29 Royal United Services Institute for Defence and Security Studies (RUSI), Occasional Paper: Cyber Insurance and the Cyber Security Challenge, 28 June 2021

30 Ibid.

- Avoiding a “race to the bottom” from competition. While competition can drive innovation and reduce costs for consumers, the cyber insurance market in the UK can be characterised as a ‘race to the bottom,’ with some insurers lowering underwriting requirements and standards to create ‘less friction in the transaction.’
- Developing consistent claim data collections to assist the development of underwriting for a still relatively immature market.
- Improving the financial viability of the cyber insurance market.

Recommendation

Insurers should collectively agree on a set of minimum-security requirements as part of risk assessments for small and medium sized enterprises (11-250 employees).

Next steps

Given the diverse range of policy stakeholders consulting on cyber issues as well as the need for engagement on key issues in international forums (in terms of standards for cyber security protection and reporting), an opportunity exists for meaningful industry-government collaboration. This would complement existing government initiatives to support business cyber protection and resilience.

In the US, President Biden in 2021 announced that the US government would work with insurers, technology companies and education institutions to define new guidelines to improve the security of the technology supply chain, noting, “The federal government can’t meet this challenge alone.” There is work being considered by our international equivalents elsewhere in relation to cyber, all indicative of an evolving area suited to a whole-of-government consideration.

[31]There are several areas of focus that need to be considered to help create a viable and sustainable cyber insurance market. Businesses, insurers and governments must work together to improvise cyber capability and resilience. Insurance companies need to have the coverage right for policies given the changing digital environment. Robust risk assessments and up-to-date analytics are vital in determining what protection a business needs. Better incident reporting, which provides insights into emerging risks, will support accurate pricing models for silent cyber and accumulation events.[32]

31 The White House 25 August 2021, *Remarks by President Biden on Collectively Improving the Nation’s Cybersecurity*

32 Forbes 25 January 2022, *The Imminent death and rebirth of cyber insurance*

Insurance Council of Australia

The Insurance Council of Australia is the representative body for the general insurance industry of Australia. Our members represent approximately 95% of total premium income written by private sector general insurers, spanning both insurers and reinsurers.

General insurance has a critical role in the economy, insulating individuals and businesses from the financial impact of loss or damage to their insured assets.

Our work with our members, consumer groups and all levels of government serves to support consumers and communities when they need it most.

We believe an insurable Australia is a resilient Australia – and it's our purpose to be the voice for a resilient Australia.

insurancecouncil.com.au