Delta Insurance Cyber Whitepaper

Issue 11 – October 2024

Embracing Cyber Risk Management

> “Cyber insurance provides a badge of quality, as it demonstrates that an insurer has assessed the insured as a good risk.”
>
> ***- MinterEllisonRuddWatts***

Contents

Major breach example and remediation. Provider shut down.

Like many cyberattacks, it started with a tiny gap in the organisation's defence.

By compromising the Citrix credentials – a remote access software – hackers gained access to the system of a national medical provider.

As the sophisticated targeted attack unfolded, it became clear that potentially hundreds of thousands of people could be affected. The hackers moved steadily throughout the organisation's data assets, successfully exfiltrating thousands of private medical records to be held for ransom. On exiting, the hackers pushed home their advantage, maximising the damage done by disabling the network.

With the initial phase of the attack complete, the medical provider's business was taken down with all network and telephony services offline. It was necessary to invoke the Business Continuity Plan, allowing some business processes for an otherwise crippled organisation to continue. A ransomware demand in the sum of millions of dollars soon eventuated.

The hackers moved steadily throughout the organisation's data assets, successfully exfiltrating thousands of private medical records to be held for ransom

Due to the critical nature of the infrastructure, the first steps towards remediation were rapid initiation of a National Cybersecurity Response.

Due to the critical nature of the infrastructure, the first steps towards remediation were rapid initiation of a National Cybersecurity Response.

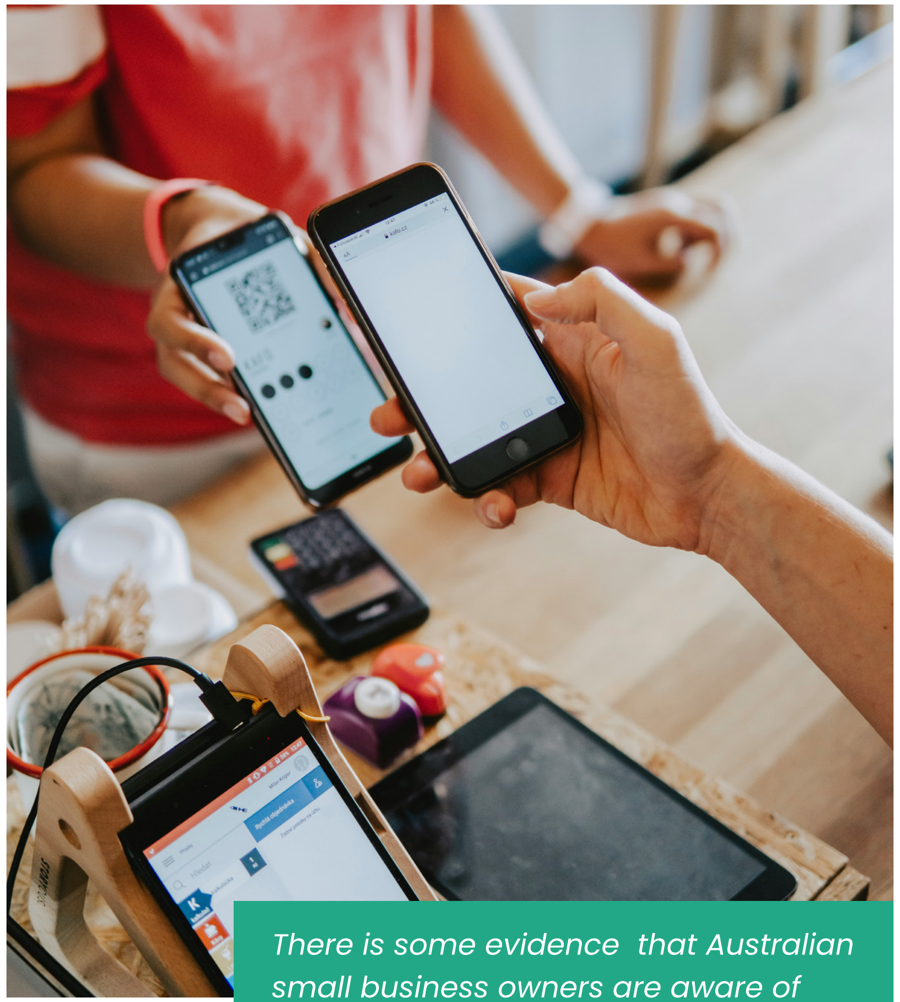
Forensic work commenced, exposing the nature and extent of the breach, and ascertaining the nature of the compromised and exfiltrated information. As a notifiable breach, in addition to alerting the authorities, all affected patients were informed of the situation.

Restoring the medical provider's information systems was the priority, with the rebuilding of servers and endpoints taking three weeks.

From an insurance perspective, challenges included the government mandating various service providers as the affected entity is a significant national organisation. This left little control over the initial response and associated costs; despite that, the Business Continuity Plan proved effective with rudimentary systems rapidly restored.

As the underwriter, Delta Insurance worked closely with relevant authorities, meeting all notification and other compliance obligations. The total sum paid out for losses incurred by the organisation amounted to nearly $1 million.

Amid changing times for cyber insurance industry, demand has never been higher.



There is some evidence that Australian small business owners are aware of cyber risk – but may not have the necessary protections in place.

When Delta Insurance released its 2018 white paper 'The Evolution of Cyber Threats: Embracing Cyber Risk Management', cyber insurance was in a nascent phase, with supply far outstripping demand.

Then, the focus from insurers was education – alerting Australian businesses to the reality of cyberthreats and the necessity for the protections offered by an integrated risk management approach in which cyber insurance plays a role.

Today, many of those dynamics have reversed: demand now outstrips supply, while some underwriters are retreating from cyber risk. Knowledge of the potential for cybercrime has improved both through the sustained efforts of the technology and insurance industries as well as general awareness driven by an increasingly digitally connected society. However, there is some evidence[1] that Australian small business owners are aware of cyber risk – but may not have the necessary protections in place.

Most business owners are also aware of cyber risk, either painfully so as the consequence of a breach suffered personally, by their own business, or through the relentless high-profile hacks that have struck major companies and organisations including DP World Australia[2], Latitude Group[3], or the incident affecting Optus which exposed up to 40 percent of all Australians' personal data.[4]

We'll explore the local cybersecurity landscape in more detail in this white paper; while the nature of cyberthreats has evolved, there has been no reduction in the severity or prevalence of attacks. This has influenced cyber insurers, too. While it is the observation of some in the technology field that poor cybersecurity posture is a sure way for a business to lose a lot of money fast, the same can be said for cyber insurers: poor pricing of risk, or poor risk assessment, loses underwriters a lot of money fast.

Today, running a sustainable and profitable cyber insurance book is more challenging than ever. Creating and delivering profitable cyber insurance solutions demands a deep and thorough understanding of both the insurance business and the technology environment.

While most underwriters have no issue with the former, the latter is a more daunting prospect: information technology is a bewilderingly complex and diverse field, with practically infinite specialisations, all of which are shot through with cyber risk. The reality is that with complexity comes opportunity for cybercriminals, who need only focus on a single weakness, exploit or hack within their area of specialty. His adversary, the defender of the enterprise (be it a major institution or a small local business) must guard against every possible potential threat. After all, the chain is only as strong as its weakest link.

This by no means indicates inability for the successful and sustainable provision of cyber insurance solutions. What it does confirm is at least two factors: one is specialisation; the other is the necessity of accurate risk assessment, including only taking on clients with demonstrably suitable cyber security postures.

In other words, businesses are only insurable if they show capable risk management, encompassing the reasonable protection (people, process, and technology) any organisation should have as a baseline measure against cyber threats.

This in turn depends on a tightly integrated supply chain, from underwriter through broker, and on to the end customer.

In addition to an assessment of the risk exposures faced by Australian organisations, this white paper examines risk management and how industry professionals can help potential cyber insurance customers secure cover as an integral component of their strategy.

Reading and sharing the information in this document is intended to help brokers and insured parties understand the risks, the realities, and the nuances so every organisation can achieve the necessary level of robust protections. This not only aids in securing cyber insurance, but also strengthens defences against incessant cyberattacks.

After all, as is always the case with cyber breaches, prevention remains a far preferable alternative to cure.

***Tesh Patel**, Managing Director,*
Delta Insurance Australia Pty Ltd

Notes from the frontline:

The broker perspective

"There's an easy calculation for anyone wondering if they should get cyber security insurance: In business? Then you need it."

*– **Lizzie Nelson***

Cyber insurance is a business necessity

Where cyber insurance was once a hard sell, today demand is almost universal. The broader market recognises the necessity for a product to help mitigate an increasingly obvious risk.

Among our client base, nearly everyone wants cyber insurance, while at the same time we constantly say not enough Australian companies have it. There's an easy calculation for anyone wondering if they should get cyber security insurance: In business? Then you need it.

Major breaches are the driving force for more people realising that if you transact online, you are at risk. Large scale hacks like Optus or Medibank make cyber risk it all more real, bringing home to the man in the street that this isn't just a commercial problem, but a risk to everyone.

This is quite distinct from the situation some 5 years ago. Then, taking cyber to market was a 'push', with many customers simply saying 'don't be ridiculous'. In one case, I recall a retailer rebuffing the idea as entirely unnecessary and even absurd.

That has changed, and by a lot. Today, recommendations of cyber insurance are well received. This may be due to increased reliance on technology systems, which is the case for a fruit and vegetable wholesaler client. This business depends on multiple interconnected systems for picking, packing, logistics, financial management and more.

The company directors recognise the existential threat posed by potential cybercrime interruptions and know their governance responsibilities extend to mitigating this risk among other ones.

Increased interest is also driven by more frequent incidences of cybercrime. There are big stories making the news, but there are also smaller stories doing the rounds at pubs and clubs, where small business owners have had to buy bitcoin and pay ransoms, rather than get on with work.

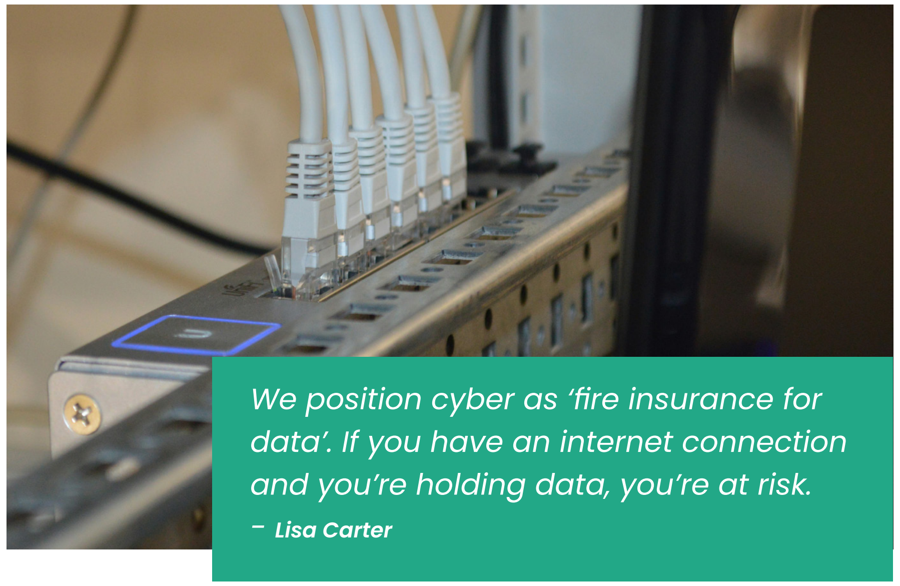
While larger companies typically have an IT person, and therefore a more thorough understanding of the risk and requirements for suitable cyber posture, it is somewhat different for the small to medium business. Typically, we share claims examples which provide context, highlight the risks and – importantly – the costs associated with cybercrime. From there, we work backwards to cover suitable for their risk profile and other requirements.

As a confluence of two complex disciplines – IT and insurance – taking cyber to market is more intensive. There is also a 'hierarchy of needs' reality to it; a business can't open shop without public liability, for example, so that's addressed first.
But there is growing urgency from organisations of all kinds with directors recognising that cyber insurance as a basic and essential cost of doing business.

*-**Lizzie Nelson**, Director,*
Insurance Mentor.

Supply constraints as demand spikes

As a company positioned as a risk advisor to our clients, there's a simple reality: cybercrime is an obvious risk for every business. It's real and very present. And as a result, we're confident in explaining its importance regardless of our client's industry. In fact, 99% of our clients have cyber insurance.



We position cyber as 'fire insurance for data'. If you have an internet connection and you're holding data, you're at risk.

*– **Lisa Carter***

We position cyber as 'fire insurance for data'. If you have an internet connection and you're holding data, you're at risk. It is not a case of 'if', but 'when' your business and cash flow is impacted. It is that simple.

However, while business customers generally are coming around to the idea and understand the necessity for cyber insurance, there is little doubt that the market is tightening. Underwriters appreciate care must be taken and as a result, capacity is retreating and appetitive for these risks is diminishing while premiums and excesses increase, often quite steeply.

Underwriters are becoming more selective of the industries and risks they will cover, with an expanding array of conditions and exclusions being applied to policies. This is due to ever-increasing losses arising out of incidents including social engineering, fraud, ransomware, or any one of a growing catalogue of existing or emerging threats.

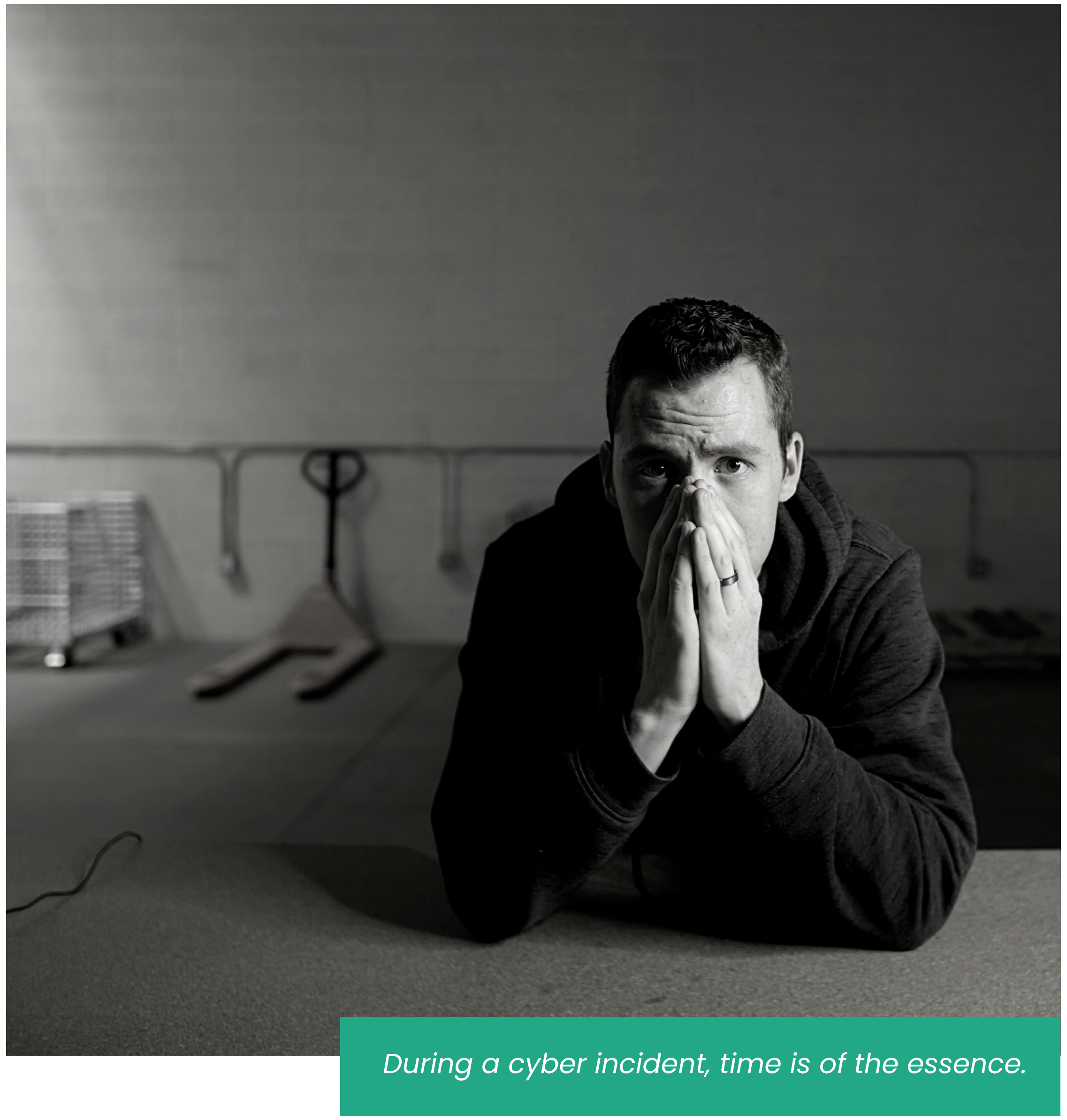
Managing risk is the responsibility of every business leader. While some of that risk is transferred to underwriters in exchange for a premium, the whole risk cannot be and is not picked up by cyber insurers. This makes clear the necessity for any organisation seeking cyber insurance to make the necessary arrangements delivering a suitable cyber security posture. This can include technology aspects, appropriate processes, and staff training.

That's why, as part of the initial engagement process, we recommend prospective clients get in touch with a specialist Managed Services Provider for assistance with preparations for a successful cyber insurance application. The application process is detailed, and any prospective client must clearly understand the questions, the disclosures, the conditions, and the coverage on offer. The client should also demonstrate sound cybersecurity measures showing awareness of the risks faced, and measures taken in mitigation of those risks.
This is essential for a favourable outcome in a market where cyber insurance is becoming an important risk mitigation tool.

***Lisa Carter**, CEO,*
Clear Insurance.

The legal perspective and framework

Common legal issues faced by entities experiencing a cyberattack



During a cyber incident, time is of the essence.

Recent large, highly publicised cyber incidents in Australia have demonstrated why organisations must carefully consider their readiness and preparedness to respond to a cyber incident. During an incident, time is of the essence.

Among the most common questions arising during a cyber incident is 'who do I need to tell, and when?' Australia's current regulatory framework provides a range of reporting obligations for Australian entities. The landscape is progressively evolving, and obligations can change depending on several factors.

Notifiable Data Breaches Scheme

Australian entities subject to the Privacy Act 1988 (Cth) (Privacy Act) have obligations in respect of an actual or suspected 'eligible data breach'. An eligible data breach occurs where there is unauthorised access, disclosure, or loss of personal information in circumstances likely to cause serious harm to individual/s, from the perspective of a reasonable person, that cannot be prevented with remedial action.

If an entity suspects it may have had an eligible data breach, it must take reasonable steps to assess whether that breach is eligible within 30 days. If eligible, the entity must notify affected individuals, and the Office of the Australian Information Commissioner (OAIC) as soon as is practicable.

Other regulatory reporting obligations

Industry bodies are increasingly becoming subject to sector-based reporting obligations. Examples include:

- Operators of critical infrastructure (including energy, transport, defence, communications, and hospitals), which must notify the Australian Cyber Security Centre of certain types of cyber incidents within 48 or 72 hours.
- ASX Listed Companies, which must notify the ASX of any incident that may have a 'material impact' on the entity's securities, or systems that may affect trade.

If an entity suspects it may have had an eligible data breach, it must take reasonable steps to assess whether that breach is eligible within 30 days.

Increasingly, downstream cyber incidents involving data disclosed to contractors are proving challenging to manage. While the organisation that 'holds' or originally collects the data typically retains responsibility for that data, the security practices, and incident response processes of their contractor can fall short of what the organisation expects. Due diligence in contractor negotiations is critical in this regard.

How to mitigate legal issues arising from cyberattacks

Preparation and proactive measures are key. While an organisation can never truly prevent an incident from occurring, consideration of the following can assist:

- *Data handling practices*: Recent cyber incidents have put a spotlight on data handling practices, including maintaining and testing security protections that are commensurate to the sensitivity of data held, and regularly assessing whether personal information remains necessary to collect, and subsequently retain.
- *Cyber incident preparedness*: All entities that deal with personal information should develop a cyber incident response plan, and regularly train staff on how to identify and escalate an incident (whether it be a small-scale data breach or cyberattack). A dedicated response team should be assigned clear roles and responsibilities that are agreed well before an incident, and the effectiveness of the plan should be tested regularly to ensure it is fit for purpose.
- *Cyber insurance*: With the costs and regulatory demands from cyber incidents increasing, cyber insurance can go some way to managing risks, and allowing access to critical support services and advice should a cyber incident occur. From a response and remediation perspective, most cyber insurance policies provide access to dedicated cyber experts across multiple fields including forensic IT, legal, and public relations management.

> *"The OAIC is increasing its regulatory focus on how entities undertake their assessments of whether an incident is an eligible data breach".*
>
> ***– Rebecca Wilson***

Challenges and opportunities

Privacy Act Reforms

The Attorney General released the Privacy Act Review Report in early 2023, with 116 proposals aimed at 'strengthening the protection of personal information and the control individuals have over their information'. On 28 September 2023, the Government announced its formal response to that report, signaling that amendments to the Privacy Act may be forthcoming in areas such as:

- introducing a statutory tort for serious invasions of privacy, a direct right of action for individuals to seek compensation for privacy breaches, and a mid-tier civil penalty regime for breaches that are not considered 'serious' or 'repeated' interferences of privacy;
- requiring small businesses, and employee records to be subject to privacy obligations (removing current exemptions); and
- narrowing the timeframe to notify of eligible data breaches.

OAIC regulatory priorities

The OAIC is increasing its regulatory focus on how entities undertake their assessments of whether an incident is an eligible data breach. Recently:

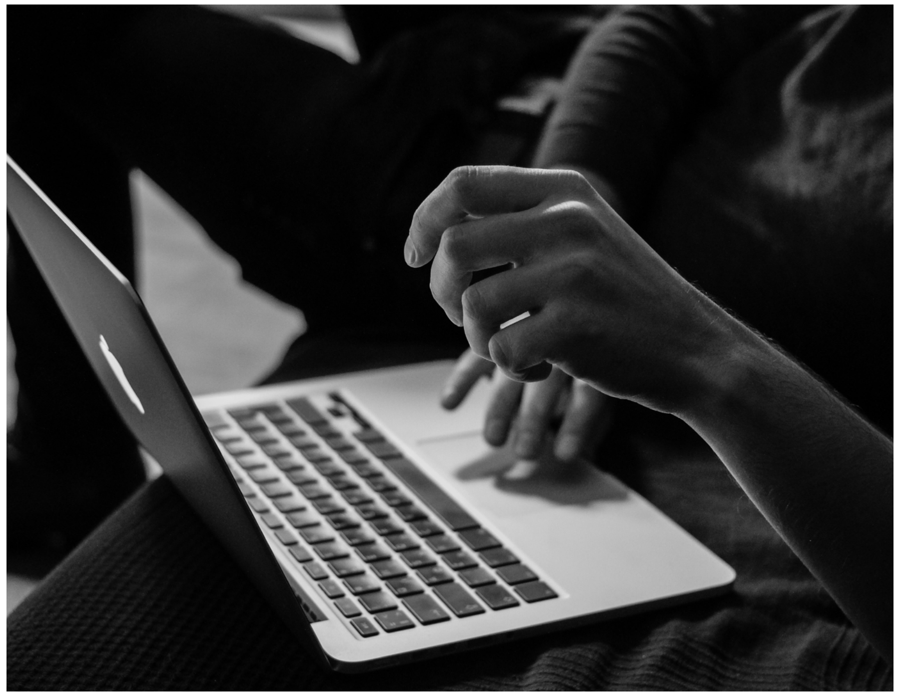
- There is an increasing trend in the OAIC taking regulatory action against entities taking too long to assess and notify eligible data breaches. Action is being taken against entities that cannot demonstrate that they took reasonable steps to finalise their assessments within 30 days. This highlights the need to have a response plan in place that has regard to this timeframe and the steps required to conclude an assessment.
- In its most recent bi-annual report into the Notifiable Data Breaches Scheme, the OAIC has encouraged entities to place more emphasis on whether there has been, or is likely to have been, unauthorised access to personal information when assessing an eligible data breach. The OAIC is warning against entities that focus on data exfiltration alone, or that conclude there has been no eligible data breach due to a lack of evidence (e.g. logs) available to clearly demonstrate threat actor activity. This can be challenging for entities which do not have mechanisms in place to capture and retain logging activities of their users (whether authorised or not).

Civil penalty proceedings

Recent court proceedings have highlighted the risks if entities do not proactively manage their privacy compliance practices. In November 2023, the OAIC commenced civil penalty proceedings in the Federal Court against Australian Clinical Labs (ACL) Limited, following an eleven-month investigation.
The OAIC alleges ACL seriously interfered with the privacy of millions of Australians by failing to take reasonable steps to protect their personal information from unauthorised access or disclosure and taking too long to assess and notify of an eligible data breach.

If the Federal Court finds there have been serious or repeated interferences with the privacy of individuals, ACL could face civil penalties of up to $2.2 million for each contravention.

> *If the Federal Court finds there have been serious or repeated interferences with the privacy of individuals, ACL could face civil penalties of up to $2.2 million for each contravention.*
>
> ***– Rebecca Wilson***



Following changes to the Privacy Act in December 2022, such serious or repeated interferences with privacy can lead to increased civil penalties of up to $50 million, 30 per cent of a company's adjusted turnover, or three times the value of any benefit obtained through a misuse of information (whichever is greater).

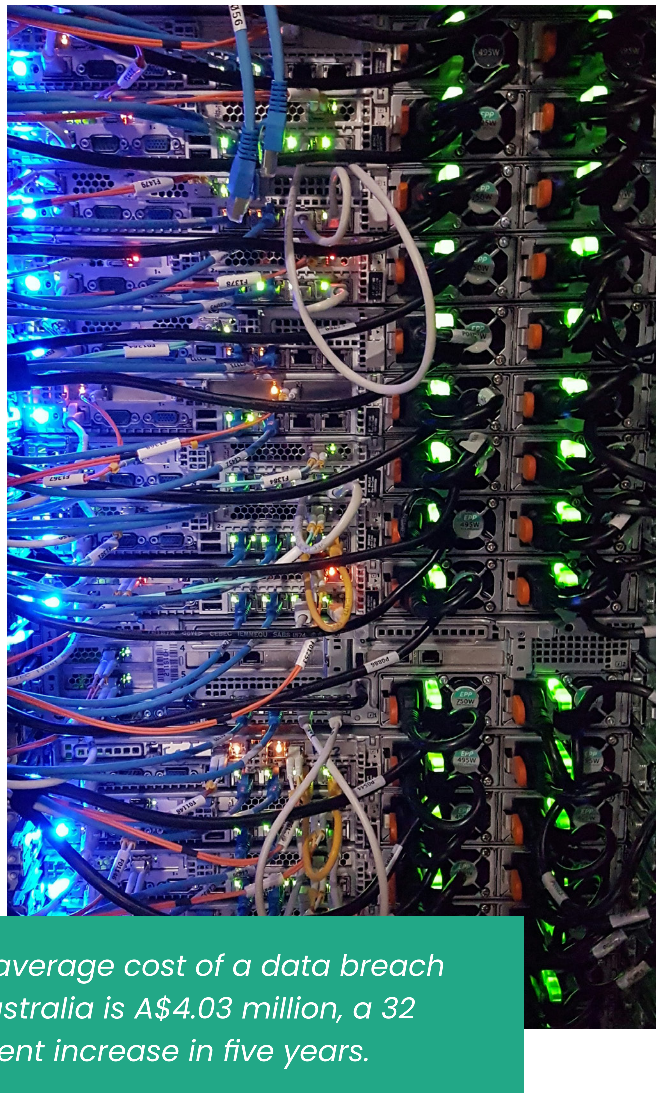
Cyber Security Strategy

The Federal Government released the 2023-2030 Australian Cyber Security Strategy on 22 November 2023, which sets an agenda for improved cyber security and risk management under six 'cyber shields'. Key areas of regulatory reform signalled under the strategy include:

- A no fault, mandatory reporting regime for ransom payments or demands;
- Single cyber incident reporting streams, and clearer guidance on what information is required from each regulatory body, that could cut down incident response times and costs for businesses;
- Enhanced cyber protections required of owners and operators of critical infrastructure and essential services; and
- Adopting uniform cyber security standards across technology and software markets, so that digital products and services are safe and fit for purpose.

***Rebecca Wilson**, Senior Associate*
Wootton + Kearney [5]

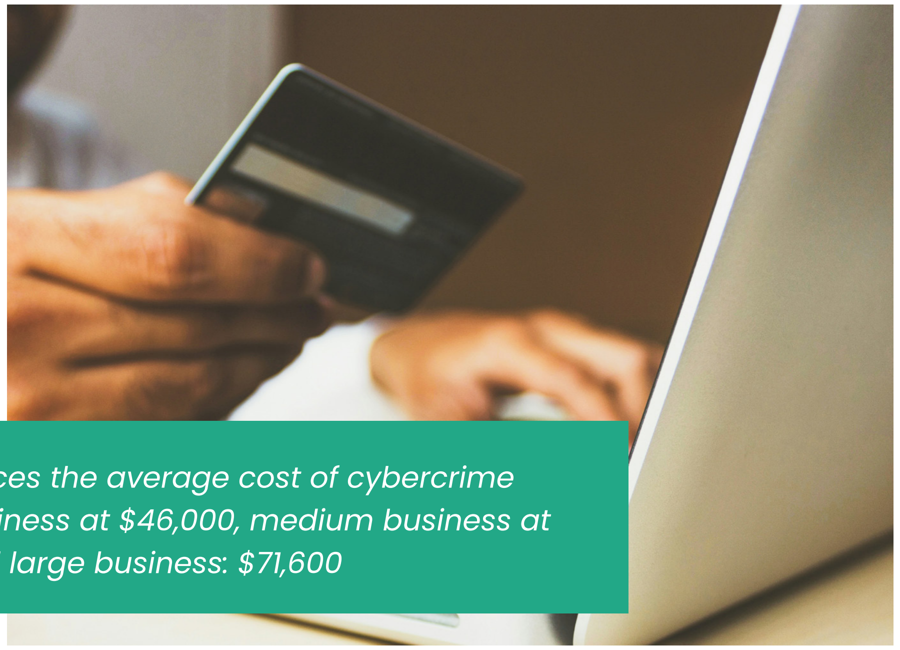
An overview of cybersecurity in Australia



The average cost of a data breach in Australia is A$4.03 million, a 32 percent increase in five years.

Known as ‘the lucky country’ with abundant natural resources, great weather, and general prosperity, Australia’s wealth has one serious drawback.

The nation’s people and businesses are a rich target for cybercriminals. This is reflected in rapidly growing incidences of cybercrime costing the nation, its organisations and citizens millions of dollars.
This is confirmed by the Australian Cyber Security Centre (ACSC) and the Australian Computer Society, which late in 2022 noted ‘Australia’s relative prosperity makes it an attractive target for cyber criminals[6]’



The ASD places the average cost of cybercrime to small business at $46,000, medium business at $97,200, and large business: $71,600

Add to that, the rollout of the National Broadband network and continuously improving cellular services resulting in an increasingly connected population puts citizens and businesses at the figurative fingertips of cybercriminals. This contributes to the bottom line for online miscreants: targeting Australian businesses and individuals pays. In fact, the Cost of Data Breach Report[7] puts the average cost of a data breach in Australia at A$4.03 million, a 32 percent increase in five years.

The frequency of attacks is relentless and increasing. The Australian Signals Directorate Cyber Threat Report 2022-2023[8] records responses to more than 1,100 cyber security incidents from Australian entities, with a separate 94,000 reports made to law enforcement through ReportCyber. This is an increase of 23 percent on the prior year.

The escalating numbers of attacks is likely owing to simple economics: hackers make money when targeting Australians. How much money? The ASD places the average cost of cybercrime to small business at $46,000, medium business at $97,200, and large business: $71,600 (note this is not specified as a ‘data breach’ as per the above referenced Cost of Data Breach Report).

These are crucial facts for brokers and underwriters alike, pointing not only to risk, but costs.

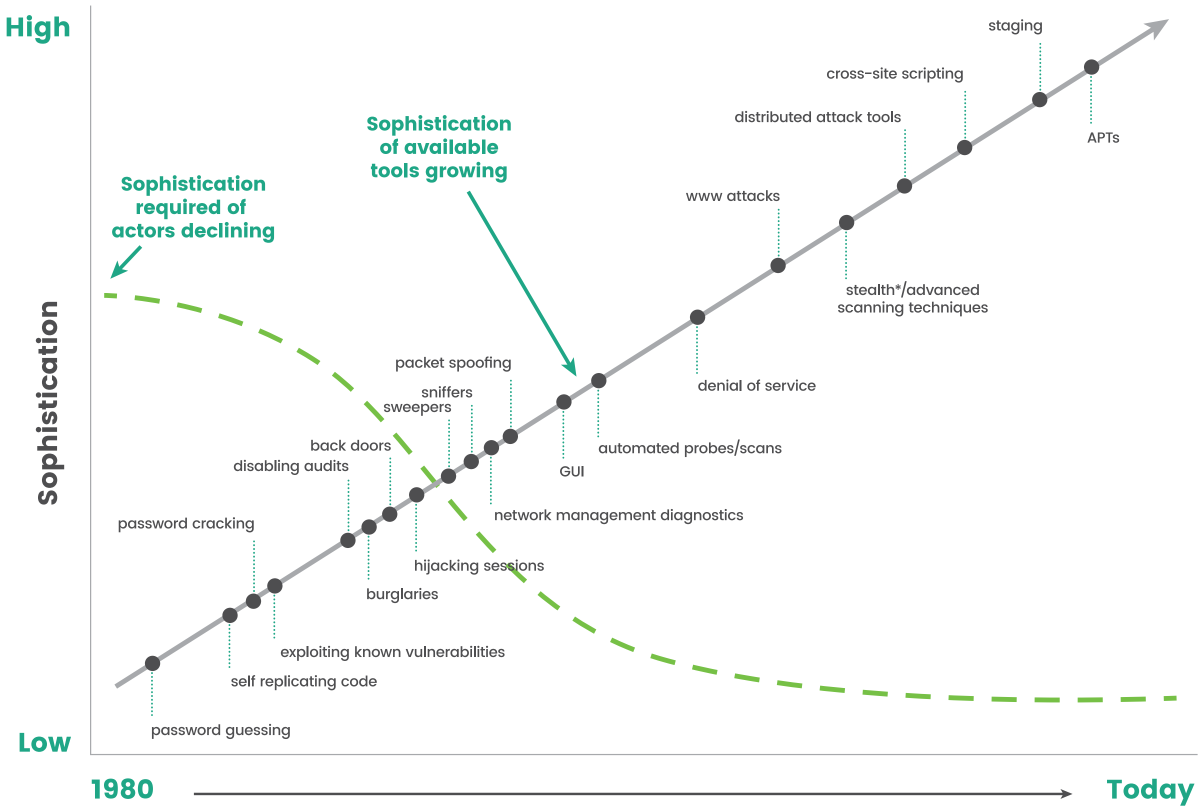
While achieving universal connectivity has proven challenging in a vast and mostly sparsely populated country, internet penetration has reached 96.2 percent with 25.31 million internet users by January 2023.

While this is a snapshot of ‘consumer’ internet use, it is relevant to cybersecurity because consumers are also the people who work in Australian industries. With estimates for the ‘human element’ being behind breaches put as high as 82% in Verizon’s 2022 Data Breach Investigations Report[9], people are almost always the weakest link, and that’s assuming technology and process aspects are sufficiently provisioned, appropriately configured, and hardened where necessary.

Moreover, several studies show that cybercriminals flourish where connectivity is universal. Commenting on its Global Threat Intelligence Report[10] BlackBerry Vice President of Threat Research & Intelligence, Ismael Valenzuela, noted several characteristics that make a country and its organizations a desirable target to threat actors. “Our research shows that there is a positive correlation between an increased number of cyberattacks and countries that possess greater internet penetration, significant economies and larger populations,” he said.

There’s a further problem. While Australians in general are growing in their awareness of the extent of cyber risks, they aren’t necessarily paying sufficient attention to the consequences. In an April 2023 report quoting data released by the ASD, The Australian Financial Review[11] notes several issues in translating awareness into meaningful action, including ‘The fact many Australian boardrooms only began to wake up to the threat of cybercrime when first Optus, then Medibank Private, were both struck by reputation-shattering data breaches towards the end of 2022’.

In other words, Australians don’t believe it will happen to them, until it does. Meanwhile, the same article quotes an anonymous source stating ‘every Australian business is being actively attacked by cybercriminals “multiple times a day”’.



Awareness is, however, improving – perhaps driven by the apparently endless news of cyberbreaches affecting everything from major corporations to private individuals.

This is a positive development. After all, 'it isn't paranoia if they really are out to get you'. While the information security industry is often pilloried for its use of 'fear, uncertainty and doubt', every internet user should have a healthy level of awareness of the reality of these risks every time they use a computer or smartphone.

A less positive development is associated with the escalating cybersecurity breaches referenced by the AFR's commentator and confirmed in the recently released ASD Cyber Threat Report 2022-2023.

The cumulative cost of those breaches to Australians and the economy is enormous, with KPMG putting the total at A$29 billion annually[12]. Notably, KPMG breaks down those costs into indirect costs which include Business Disruption (40 percent), Information Loss (29 percent), Revenue Loss (25 percent), Productivity Loss (29 percent), and Equipment Damage (4 percent). This confirms that aside from financial loss from theft or extortion, the impact of a cyberattack goes further. While prevention is always better than cure, it is an uncomfortable reality that even the most prepared, most cyber-aware and most secure organisation can fall victim to an attack.

Types of attacks and perpetrators

The barrier to entry for cybercriminals is low. Perpetrators range from mischief-making teenagers through to sophisticated, well-organised and well-funded criminal groups structured and operating like a business.

Even entire nations are targeted with state-sanctioned attacks as part of espionage or cyber-warfare initiatives (though this falls outside the scope of this white paper).

The tools used by cybercriminals are readily available on the 'dark web', as is support, encouragement and assistance from similarly minded criminals acting in concert online. The cost of cybercrime tools, or even the cost of hiring someone to perform a cybercrime 'as a service', is astonishingly low. Cybersecurity tools vendor CrowdStrike reports that Ransomware as a Service is available from as little as US$40[13].

This is confirmed in the Sophos 2023 Threat Repor[t14], the conclusion of which notes: that there has been "... the continuous lowering of barriers to entry for would-be cybercriminals and the commodification of what once would have been considered "advanced persistent threat" tools and tactics. While there has long been a thriving marketplace for hacking tools, malware and access to vulnerable networks, the lessons learned from the recent history of ransomware operations and other well-funded malicious actors are more rapidly becoming available to the wider criminal community—as are commercial security tools designed to defeat some defenses..."

The methods, techniques, tools, and tactics used by cybercriminals are numerous, ever-expanding, and constantly evolving. TechTarget[15] lists at least 13 types of attack; knowing what these attacks are and how they work is highly recommended for every broker; recognising and understanding cybercrime attack methods helps identify and avoid becoming a victim and informs a risk management mindset.

As new tools emerge, hackers adopt them – often faster than commercial organisations can, because the 'product development' lifecycle for those operating outside the law is untrammeled by quality control, health and safety, and so on. Hackers and information security professionals have long engaged in an 'arms race', each seeking the advantage of a new technology or technique before the other can. The emergence of artificial intelligence is being used by both sides[16]. While 'ethical programming' sets out to limit its express use for nefarious purposes, platforms like ChatGPT are likely being used by hackers to accelerate malware development.

Whether targeting individuals or businesses, the types of attacks include: the use of various types of malware (prominently including ransomware); multiple methods targeting passwords and identity to gain unauthorised access; Distributed Denial of Service which aims to interrupt crucial services; various forms of phishing; methods targeting databases (such as SQL injection); cross-site scripting which compromises websites; man-in-the-middle attacks which intercept messages between two parties; DNS spoofing to fool people with fake sites; botnets; watering hole attacks, and insider threats.

These methods are often used combined, with the goal of extracting valuable information (often usernames and passwords, or banking PIN numbers) for later use to extract money or extract more information for use as a ransom.

The tools used by cybercriminals are readily available on the 'dark web', as is support, encouragement and assistance from similarly minded criminals acting in concert online.

Any one of multiple threat reports widely available from security technology vendors, government organisations, research companies, and others confirms an escalating threat environment along with rising costs of effective protection.

The Kaspersky Security Economics Repor[t17] quantifies the costs, with its key findings including:

- Cybersecurity budgets in 2022 averaged $3.75m for enterprises and $150k for SMBs. Both segments are planning to increase budgets equally by up to 14 percent in the coming year.
- Communications, product development and customer support are the top three processes most affected by cybersecurity intrusions.
- Data leaks were the most encountered security issue in 2022. This type of incident was most often caused by employees (22%) and attackers (23%).
- Delivering cybersecurity solutions and efficiencies by bringing in external experts are the main drivers leading companies to outsource IT security.

In short, cybersecurity risks and costs are real and substantial. Providing cyber insurance cover sustainably therefore depends on a cautious, risk-management approach where underwriter, broker and customer work together towards the common goal of quantifying and mitigating cyber risk, v insurance one component in a broader cyber resilience strategy. The Actuaries Institute of Australia[18] notes, 'While the first line of defence against cyber risk will always be good cyber hygiene and security, cyber insurance is an important second line of defence.'

Cybersecurity insurance demand is up as supply recedes

Demand for cyber insurance is increasing substantially around the world and in Australia itself. The reasons are simple: significant threats and significant losses in the event of a hack.

Despite the differing views on long term growth, what is clear is that cyber insurance is a potentially lucrative market.

There is also increased awareness of the availability of insurance protection to cover the impact of cyber events/ intrusions. However, even as demand spikes, supply is receding. Providing sustainable and profitable cyber insurance isn't easy and depends on appropriate knowledge and insight into the complex world of information technology as well as business.

A Fortune Business Insights paper[19] anticipates growth in the global cyber insurance market at a CAGR of 25.7% between 2022-2029, increasing from US$12.83 billion to US$63.62 billion in gross written premium; the paper notes increasing incidences of hacking resulting in fines and other punitive measures from governments for customer data breaches. It also points to the reality of small and medium businesses coming into the crosshairs of attackers. Research and Markets[20] offers a slightly less rosy forecast and assesses the value of the global market considerably lower, at US$7.06 billion in 2020. It anticipates growth to US$20.43 billion in 2027.

Despite the differing views on long term growth, what is clear is that cyber insurance is a potentially lucrative market. While the first such products emerged in the 1990s, the appeal of and necessity for cyber insurance has escalated in recent times (and indeed it has escalated dramatically since Delta Insurance entered the Australian market in 2022).

However, many insurers are realising that the rich market value and double-digit growth figures are far from easy money. The utmost care is required in providing cyber insurance; as payouts increase, supply is dwindling, coverage terms are becoming more restrictive, and premiums are escalating. (Careful insurers running a profitable book, it should be noted, are less likely to increase their premiums, though these premiums were likely comparably high in the first instance, reflecting the substantial due diligence invested into every policy). In fact, an April 2022 Fitch Ratings report found that cyber premiums rose by 74% in 2021.

With the increase in cyberattacks has come an increase in insurance payouts. Insurance companies are increasing premiums to keep up. A more recent CNBC report[21] confirms that rising premiums along with reduced supply may make cyber insurance unaffordable for some companies.

In Australia, the situation mirrors that in the rest of the world. Cyber breaches are increasingly common; it isn't just the high-profile ones like Optus or Medibank which make the news, but many smaller heists are also affecting small local businesses. Awareness is heightened, most people know someone who has been hit, or may even be a victim of ransomware or other hacks themselves.

At the same time, demand is up, and insurer's risk appetite is reducing. General insurers are showing increasing caution, as the costs of providing effective cover to the mass market aren't economical. This is causing a 'flight to specialisation'. Some coverage is more difficult to find, and it is harder for local businesses to secure cyber insurance. In other areas, such as state-sponsored cyberattacks, coverage is being withdrawn altogether, starting in 2023, Lloyd's of London requires exclusion of catastrophic state-backed hacks from standalone cyber insurance policies[22].

> *"IT departments may realise as they work through the questions that the answers they would give will not satisfy insurers, so it may be necessary to take remedial steps urgently so that a more satisfactory response can be given".*
>
> ***– MinterEllisonRuddWatts***

Cybersecurity posture will impact cover

Leading New Zealand law firm MinterEllisonRuddWatts notes in an online pape[r23] that securing cyber insurance is getting harder. "Insurers are responding to the rising risks and costs of cyber events with increasingly detailed assessments of insureds' IT systems, while in some cases also reducing cover limits and increasing premiums… [others] have reduced limits significantly or withdrawn cover altogether. Large firms, such as those with revenue over NZD$100 million, are facing particular scrutiny, as they present an increased perceived risk as more attractive targets to criminals", wrote MinterEllisonRuddWatts.

The law firm further advised, "The complexity of insurers' questionnaires and their importance means that IT departments must be well prepared and resourced to answer them. This should be done well in advance of the cyber insurance renewal date, as the time commitment is significant, and answers often need to be drawn from different sources. IT departments may realise as they work through the questions that the answers they would give will not satisfy insurers, so it may be necessary to take remedial steps urgently so that a more satisfactory response can be given".

Echoing MinterEllisonRuddWatts, in a March 2022 Consultancy.com item[24] BeyondTrust director Scott Hesford notes a tactical retreat. 'Insurers are tightening underwriting guidelines and mandating their customers have certain security controls in place, such as privileged access management. They are also becoming more selective about who they are willing to cover. Just as a driver who is involved in multiple accidents may be dropped by their insurer, the cyber insurance market is no different. From an insurer's standpoint, not every applicant is a good candidate.an expert warning that premiums may become unaffordable'.

Any business seeking cyber cover is well-advised to consult with an IT provider with proven cybersecurity capabilities ahead of seeking new coverage or in conjunction with the insurer.

Controls typically assessed by brokers and underwriters include:

- Multifactor authentication for remote access and admin/ privileged access.
- Endpoint Detection and Response (EDR).
- Secured, encrypted, and tested backups.
- Privileged Access Management (PAM).
- Email filtering and web security.
- Patch and vulnerability management.
- Cyber incident response planning and testing.
- Cybersecurity awareness training and phishing testing.
- Hardening techniques including Remote Desktop Protocol (RDP) mitigation.
- Logging and monitoring/ network protections.
- End-of-life systems replaced or protected.
- Vendor/digital supply chain risk management.

In providing cover, complete assessments of the cyber security posture of the client are necessary before writing any policy. Hesford adds, 'Qualification for cyberattack coverage is being carefully assessed and potentially denied based on the answers of prospective and current customers to comprehensive security questionnaires. Insurance companies are also increasingly hiring security professionals to help them navigate the path to insuring qualified customers and denying those who don't qualify or otherwise pose too big a risk'.

Any business seeking cyber cover is well-advised to consult with an IT provider with proven cybersecurity capabilities ahead of seeking new coverage or in conjunction with the insurer. The process of testing the market for cover can itself contribute to an improved security posture, as cover will only be extended if risks are suitably quantified and appropriately mitigated through demonstrable plans, measures, processes, technology, and personnel.

MinterEllisonRuddWatts makes further valuable observations. "While cyber insurance is increasingly challenging to obtain, brokers report that it continues to benefit insureds. They report that, perhaps because of the care taken when it is arranged, it features a relatively high claim acceptance rate compared with other types of insurance, so notwithstanding the cost and time investment required, it is worthwhile and provides a real benefit.

"Cyber insurance also remains one of the few insurance products that assists insureds to prevent claims. Insurance assessments are often valuable tools to identify security weaknesses and remedy them, as insurers often have up to date knowledge of the latest risks. Cyber insurance discussions can therefore benefit insureds by assisting them to improve their systems and remove vulnerabilities."

And once secured, cyber insurance offers value beyond the cover itself, says the law firm. "Cyber insurance provides a badge of quality, as it demonstrates that an insurer has assessed the insured as a good risk."

Providing cyber insurance isn't a fast, simple transaction. Instead, it rests on considerable expertise, has a long sales cycle, and requires working closely with your customers and your underwriter.

A lucrative market for specialists

It is clear from multiple threat reports that the risk environment for all business types is escalating.

Cybercriminals operate somewhat indiscriminately from the safety of geographically distant locations, often with little or no fear of consequences from law enforcement.

Their organisations and activities are profitable, adding impetus and emboldening their activities. The barrier to entry for new cybercriminals is low, while their reward potential is high, further heightening the threat environment for every legitimate business. Meanwhile, Australia's connected population and somewhat relaxed attitude to cyber threats make it an enticing target.

Providing cyber insurance isn't a fast, simple transaction. Instead, it rests on considerable expertise, has a long sales cycle, and requires working closely with your customers and your underwriter. However, for those brokers who choose to specialise and work with an increasingly circumspect group of cyber underwriters which have the necessary knowledge, experience and track record in delivering sustainable solutions, substantial rewards await.

What is clear is that caution is advisable from brokers and underwriters, who must accurately assess and gauge risk before writing policies. By the same token, organisations seeking cyber security cover are well-advised to seek the advice and guidance of their IT providers – including cyber security specialists.

While capacity is retreating and is likely to continue doing so, Australia's business owners are still well positioned to secure cybersecurity cover. However, this is only possible for those organisations demonstrating an appropriately rigorous, proactive, and comprehensive approach to risk mitigation.

About Delta Insurance

Delta was established in 2014 to answer the call for insurance in new or specialised areas, with exceptional customer service – all underpinned by transparency and integrity.

Today we cover over 30,000 risks in New Zealand, Singapore and Australia. We are proud to have won ANZIIF's Insurance Underwriting Agency of the Year award in New Zealand for the last five years for our continued focus on our customers. As well as resolving claims, we focus on prevention using a range of risk mitigation strategies, partnerships and solutions.

delta

Our Philosophy

Our Vision
We embrace change to make the world a safer place.

Our Mission
We give you the confidence and security to succeed.

Our Values
With our entrepreneurial spirit, we're proactive and nimble. We do the right thing. We're passionately curious. We're at our inspirational best when we collaborate. We enjoy the journey and celebrate it.

Sources

1 https://www.cyber.gov.au/sites/default/files/2023-03/2023_ACSC_Cyber%20Security%20and%20Australian%20Small%20Businesses%20Survey%20Results_D1.pdf

2 https://edition.cnn.com/2023/11/13/tech/australia-dp-world-cyberattack-ports-intl-hnk/index.html

3 https://www.reuters.com/technology/australias-latitude-group-says-customer-information-stolen-cyber-attack-2023-03-15/

4 https://www.bbc.com/news/world-australia-63056838

5 Sources:
https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report

https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

https://www.asx.com.au/documents/rules/Guidance_Note_8.pdf

https://www.cisc.gov.au/resources-subsite/Documents/cyber-security-incident-reporting.pdf

https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

https://www.oaic.gov.au/newsroom/oaic-commences-federal-court-proceedings-against-australian-clinical-labs-limited

https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2023

https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-2-preparing-a-data-breach-response-plan

https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme

https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information

6 https://ia.acs.org.au/article/2022/australia-s-wealth-makes-us-a-cyber-target.html

7 https://mysecuritymarketplace.com/reports/cost-of-data-breach-report-2023/

8 https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023#

9 https://www.verizon.com/business/resources/reports/dbir/

10 https://blogs.blackberry.com/en/2023/02/top-10-countries-most-targeted-by-cyberattacks-2023-report

11 https://www.afr.com/technology/why-australia-is-such-a-juicy-target-for-cybercriminals-20230404-p5cxvn

12 https://assets.kpmg.com/content/dam/kpmg/au/pdf/2023/cost-of-cyber-attacks-australia.pdf

13 https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

14 https://www.sophos.com/en-us/content/security-threat-report

15 https://www.techtarget.com/searchsecurity/tip/6-common-types-of-cyber-attacks-and-how-to-prevent-them

16 https://www.techopedia.com/ai-in-cybersecurity-the-future-of-hacking-is-here/2/34520

17 https://calculator.kaspersky.com/

18 https://actuaries.asn.au/public-policy-and-media/thought-leadership/green-papers/cyber-risk-and-the-role-of-insurance

19 https://www.fortunebusinessinsights.com/cyber-insurance-market-106287

20 https://www.researchandmarkets.com/reports/5636783/global-cyber-insurance-market-forecasts-from

21 https://www.cnbc.com/2022/10/11/companies-are-finding-it-harder-to-get-cyber-insurance-.html

22 https://www.wsj.com/articles/lloyds-to-exclude-catastrophic-nation-backed-cyberattacks-from-insurance-coverage-11660861586

23 https://www.minterellison.co.nz/insights/cyber-risk-and-cyber-insurance-themes-and-predictions

24 https://www.consultancy.com.au/news/5111/why-securing-cyber-insurance-coverage-is-becoming-more-challenging

delta