Colton Computer Technologies

NLT INSURANCE BROKERS

YOU'VE GOT THIS.

A straightforward guide to cyber insurance.

THE WHY, WHAT, AND HOW.

Contents

When it comes to cybercrime, you can't keep your head in the sand forever. Here's why.

Understandably, the thought of cyber insurance (and all the requirements that go with it) makes many business owners nervous.

While it can be tempting to ignore cybercrime and all the damage it does, it's a problem that's not going to go away anytime soon. And given the potential losses and penalties, you can't afford to put cyber insurance in the too-hard basket.

It's fair to say that Australia is behind the game when it comes to cyber insurance.

The **Insurance Council of Australia** (quoting Lloyds of London) reports that Australian businesses are significantly underinsured for cyber risk, with only about 20% of SMEs and 35-70% of larger businesses having standalone cyber insurance. By comparison, they say, "cyber insurance products first developed in the United States of America (US) in the late 1990s and the US still accounts for about 90% of the global cyber insurance market."

We've written this guide to help demystify what cyber insurance is, why you may need it, and, critically, how you can keep those premiums down (and de-risk your business) by tightening up your cybersecurity posture.

First, though, let's look at some of the facts.

1. Just being in business is increasingly (cyber) risky

The very latest **ASD Cyber Threat Report 2022-2023** reports that "Malicious cyber activity continued to pose a risk to Australia's security and prosperity in the FY 2022-23. A range of malicious cyber actors showed the intent and capability needed to compromise vital systems, and Australian networks were regularly targeted by both opportunistic and more deliberate malicious cyber activity."

ASD says they responded to over 1,100 cyber security incidents from Australian entities. Separately, nearly 94,000 reports were made to law enforcement through ReportCyber – around one every 6 minutes (it was one every 7 minutes the year prior).

The top 3 cybercrime types for businesses between 2022 and 2023, says ASD, were email compromise, business email compromise (BEC) fraud, and online banking fraud.

2. The cost of being vulnerable to cybercrime is increasingly expensive

Along with the high volume of reported cybercrime incidents, **ASD** reports that over the last year, the average cost of cybercrime per report went up 14%. That translates to:

- Small business: $46,000 per report
- Medium business: $97,200 per report
- Large business: $71,600 per report

And then, there are the increasingly stringent government-imposed fines for failing to protect your data and your customers. The **Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022** increased the maximum penalty for serious or repeated privacy breaches from $2.22 million to whichever is the greater of:

- $50 million
- 3x the value of any benefit obtained through the misuse of information; or
- 30% of a company's adjusted turnover in the relevant period.

3. Small and medium businesses are vulnerable and underdefended

In their article, "Australia—Small businesses vulnerable to rising cybercrime," Export Finance Australia – Australian Government says that SMEs face **significant risk** and that 43% of cyberattacks are aimed at small businesses.

ACSC's **Cyber Security and Australian Small Business** reports concluded that SMEs are also less prepared to defend themselves against cyberattacks; nearly half (48%) of Australian SMEs spend less than $500 annually on cybersecurity.

The **Australian Small Business Ombudsman** reports that more than 60% of Australian SMEs hit by a cyberattack or data breach **do not** survive the incident.

What is cyber insurance?

It's likely that you already have business liability, commercial property, errors and omissions (E&O) insurance, and more. The good news is that many of the same trusted providers of these products also sell cyber insurance policies.

Most cyber insurance policies include:

- First-party coverage - which applies to losses that directly affect your business
- Third-party coverage - which applies to losses suffered by others from a cyber event or incident based on their relationship with your business

What losses and costs do cyber insurance policies generally cover or help with? (This will vary depending on the package you select.)

- The financial losses resulting from cyber events and incidents, including recovering the lost revenue and ongoing expenses experienced during the downtime
- The costs associated with remediation – which can include paying for legal assistance, cybercrime investigators, crisis ommunicators, customer credits or refunds, and implementing measures to mitigate further damage.
- Coverage for ransomware and extortion payments and the expense of responding to ransom demands.

As a small-to-medium business, do you need cyber insurance?

Regardless of size or industry, if you're a victim of a cyberattack and your data is lost or compromised, you stand to lose:

- Your reputation
- Your customers
- Your hard-earned revenue

And, of course, you could face liability for damages stemming from the theft of 3rd party data.

It may be tempting to feel that as a small or medium business, you are a much less attractive target for cybercriminals. However, the reality is that as larger organisations and enterprises have the capability and budget to invest in comprehensive and robust cybersecurity solutions and services, by default, you become an easier target.

Australian Cyber Security and Home Affairs Minister **Clare O'Neil** observed that while large businesses received some of the biggest cyberattacks, they typically recovered - but "attacks on small and medium-size businesses could be terminal."

In its **Cybercrime in Australia 2023** report, the Australian Institute of Criminology (AIC) found that small-to-medium businesses experience a range of harms from cybercrime that extend beyond financial costs, such as impacts to personal health and legal issues.

Your 'do I need insurance?' checklist:

Even if you feel you are well prepared for a cyberattack, it's unwise to assume that you don't need cyber insurance.

However, very few small businesses are as ready as they think they are – and some don't have any plan in place at all.

Does this sound like you?

- You create, store, and manage electronic data online
- You store customer contacts, customer sales, personally identifiable information, and credit card numbers
- You are an e-commerce business, and your sales and customers can be impacted by your website going down
- You store customer information on your website
- The customer data you store is commercially or personally sensitive (and therefore of high value to cybercriminals)

All the above make you attractive to cybercriminals. And whether it's through a direct attack on your network or via your employees or their endpoint devices, the bad guys are relentless.

No industry is safe. Recent **research** by a leading insurer advises that the average cost of a cyber insurance claim for the construction industry is $312,000; for real estate organisations - $230,000; for financial services organisations - $225,000; and for not-for-profits - $165,000.

Is your business protected from these common threats?

The list of common cyberattacks grows yearly. They're big business for cybercriminals, to the extent that attackers can now subscribe to ready-to-use ransomware as a service (along with support desks and upgrades) – much as you'd subscribe to any useful online service. With the addition of artificial intelligence to the cybercriminal arsenal of tools, it will become even more challenging to avoid, resist, or recover from an attack.

These are just some of the forms of attack you will likely experience over the coming year:

1. **Ransomware attacks.**
   While ransomware may seem like old news, according to the **ASD Cyber Threat Report 2022-2023**, it is the most destructive cybercrime threat to Australians. Scarily, Microsoft says that **96.88%** of all ransomware infections take under four hours to successfully infiltrate their target (some take as little as 45 minutes to take over your network).

2. **Social engineering and human error.**
   With highly effective tactics such as social engineering (phishing, email impersonation, stolen credentials, ransomware, and more), criminals rely on the vulnerability of your people rather than the weaknesses in your security systems. And if you think it's hard to fool people, **Verizon's Data Breach Investigations** report that 85% of all data breaches involve human interaction.

3. **Third-party exposure.**
   Third-party networks can be the weakest link in your own cybersecurity defences, offering a sly foot in the door to an otherwise well-protected environment. Or your own network vulnerability and privileged access can offer an easy way into the systems of those you do business with.

4. **Configuration errors.**
   Whether you've set up your system in-house or are using a partner, configuration errors seem to be a fact of life. According to OWASP (the Open Worldwide Application Security Project), they found some form of misconfiguration in **90%** of the applications they examined.

5. **Inadequate cyber hygiene.**
   From using unprotected Wi-Fi networks in cafes, hotels, or public spaces to reusing the same predictable passwords, to not requiring multi-factor authentication, to using unprotected devices, businesses make it all too easy for cybercriminals to leverage poor cyber hygiene habits.

6. **Cloud vulnerabilities.**
   We assume that due to the level of investment, the cloud is inherently safe. But the opposite is true, with IBM reporting that cloud vulnerabilities have increased **150%** in the last five years.

7. **Mobile devices under attack.**
   With so many working-from-home and bring-your-own-device (to work) policies, there's been an upsurge in security incidents where employees download malicious mobile apps – which enter your network. Security magazine reports that "the average user is six to 10 times more likely to fall for SMS phishing attacks than email-based attacks" and that, as of 2022, malware is detected on one out of every 20 Android devices.

What is clear is that as the threat landscape continues to grow, so must your investment in cybersecurity and insurance.

Gearing up for cyber insurance

To qualify for cyber insurance, you need to have specific cyber protection measures and controls in place. You will also be required to provide detailed information on the value of your clients, previous attacks, backup regime, endpoint, and network security, and much more.

Here's an overview of the type and depth of information you will be expected to provide:

Revenue

- Annual revenue
- Revenue by state or territory

Details of previous cyber incidents

- Description and date of incidents
- Financial impact
- Mitigating steps to avoid future incidents
- Any current risk factors that could give rise to a Data Breach or Cyber incident

IT infrastructure and resourcing, including:

- Managed service provider
- Number of servers on your network
- Number of desktops and laptops
- Annual IT budget
- Percentage spent on IT security
- Any third-party technology partners for IT Infrastructure

Data storage and management

- Data types
- Data protection measures (access controls, encryption, network segmentation, etc.)
- Deletion of old records
- Storage, frequency, and testing of backups
- Number of backup copies and how you prevent multiple copies from being impacted by the same event
- Recovery time

Endpoint security

- The Endpoint Protection and Endpoint Detection and Response you use on your network
- How these products are monitored and managed
- Whether they cover all endpoints on your network

Perimeter security

- Next-generation firewalls in use
- Regularity of vulnerability scanning of network perimeter
- Frequency of penetration testing of network architecture and whether a third party conducts this
- Multi-factor authentication for remote access to your network
- Methods to secure remote access to your network

Email security

- Multi-factor authentication for remote access to company email accounts
- Use of emailing filtering software

Network security

- How you protect privileged user accounts
- Whether non-IT users have local administrator rights on their computer
- Use of a network monitoring solution to alert you to malicious/suspicious behaviour
- Use of a Security Operations Centre (SOC)
- Whether you have any end-of-life or end-of-support software
- Patch management process to ensure critical patches are applied in a timely process
- Significant changes planned for your IT infrastructure

Staff training

- Phishing testing
- Responsible password practices
- Cyber best practices
- Cyber incident response preparedness
- Additional controls that you use
- Audit information
- Procedures around intellectual property
- Legal counsel relating to privacy policy, terms of use, terms of service and customer policies

Why all the questions?

While the above list may seem daunting, your insurer wants to know that you are doing the best you can to protect your business, your employees, and your customers.

Plus, going through each item reminds you what you should be doing (and regularly reviewing) as a matter of best practice – regardless of how large or small your business is. And if you don't have one already, it's a great starting place for a cybersecurity plan.

Here's a quick plain language recap of why each point is important to your business – and your insurer:

Data storage and management:
Your business will take a significant hit if you lose or can't access your data. You are legally responsible for protecting client data – and the fines for failing to do so are significant. You need to know that in case of natural disaster, or a ransomware attack, that you can recover your data from your backup system and get back to work as quickly as possible. Your data protection and recovery processes go a long way towards ensuring your business is resilient and able to resume operations as quickly as possible.

Endpoint security:
If, like most businesses, your team use a wide range of endpoint devices (from mobiles, to tablets, to desktops) to access your systems, it's critical those devices are protected. Your insurer wants to know that you've taken every step to monitor and manage these devices as it reduces the opportunity for cybercriminals to freely access your network via an unsecured and forgotten side door (like your son's old iPad).

Perimeter security:
Think of perimeter security as your first line of defence. It's the virtual barbed wire fence and constantly patrolling dogs tasked with protecting and deterring criminals from attempting to access to your valuable systems. It includes gate guards who require those wanting to gain entry to validate their identity using multifactor authentication.

Email security:
Email remains a key method of network entry and infiltration by cybercriminals. Remote email access is a point of vulnerability, so multi-factor authentication is important. Email filtering software helps weed out and block suspected attempts to insert dangerous code into your system via apps, PDFs, false website links and more.

Network security:
From protecting privileged user accounts (like system administrator) to making sure the right people have the right admin rights on your system, your network needs to be protected, maintained and vulnerabilities (known weaknesses) patched as soon as possible. The more rigorous your processes and better your systems, the safer your network is.

Staff training:
People remain both your best defence against cybercriminals and your greatest weakness. This means that training them to recognise potential attacks through emails, SMS, or even phone – is critical. It also means resetting old habits like reusing passwords, using common passwords (123456), or storing them on sticky notes. Just like in a civil defence emergency, they need to know how to recognise an attack, and what to do. A good training program will include ongoing refreshers and random tests.

How can you reduce your cyber insurance premiums?

As with any insurance, keeping your risk profile low is the best way to avoid attracting higher premiums.

While the list of preventative measures is long, it includes the basics of minimising risk through cyber awareness training, ensuring you aren't bypassing multi-factor authentication, following best practice checks and double checks before paying invoices, patching vulnerable software applications promptly, implementing password security standards, and having a backup program in place. And if you've already had an incident, taking the necessary steps to mitigate a repeat occurrence.

Insurance companies look for ongoing improvement in your risk posture and evidence that you've learned from your mistakes.

What insurance package is for me?

Most insurers offer a range of cyber insurance options, generally falling into the simple, popular, and comprehensive categories.

Cyber insurance generally covers you for losses caused by:

- Data breaches
- Ransomware and malware
- Cyberattacks
- Employee misadventure or negligence
- Multi-media liability
- Privacy breaches
- Loss of service
- Damage to your systems

What's not covered? A drop in the value of your business due to an incident, for example, the theft of intellectual information, is usually exempt.

Summary

Complacency is a dangerous thing. In today's world, 'she'll be right' is a high-risk approach to protecting everything you've worked so hard for.

While cyber insurance may pose some challenging requirements for those who've never considered themselves at risk, the checklist on page 5 is also a great best practice guide to getting your cyber security up to standard. So, if you do experience an incident, you know you can recover.

We certainly hope you'll never need to make a claim.

But if 43% of cyberattacks in Australia are aimed at small businesses, it's more than likely that at some stage, you will fall victim to the bad guys. However, with the right managed cyber security services and cyber insurance partners by your side, your chances of coming out of it - reputation and bank balance intact - are far greater.

To find out how to cyber-secure your business, contact:

Colton Computer Technologies

✉ sales@colton.com.au
☎ 02 6361 1116

To protect your business from the financial fallout of a cyber-incident, contact:

NLT Insurance Brokers

✉ levi.thurston@nltinsurance.com.au
☎ 02 6331 0227

About Colton Computer Technologies:

Colton Computers provides relevant, reliable IT and telephony solutions empowering small business for the Central Tablelands and Central West of New South Wales.

By partnering with customers and building strong, long-term relationships, Colton enables businesses and organisations to leverage the technology available to maximise efficiency, productivity, and cyber security in the workplace.

Colton Computer Technologies
coltoncomputers.com.au

About NLT Insurance Brokers:

Based in the Central West of NSW, NLT Insurance Brokers Pty Ltd has over a decade of experience in insurance and financial services. We provide exceptional personal service and competitive premiums.

We specialise in cyber, business, construction and trades, farm, house and contents, motor vehicle and professional insurance.

NLT
INSURANCE
BROKERS