WHITE PAPER

PRORISK

8 ways to protect your small business from Cyber attacks

Our guide to helping small to medium sized enterprises increase their cyber resilience.

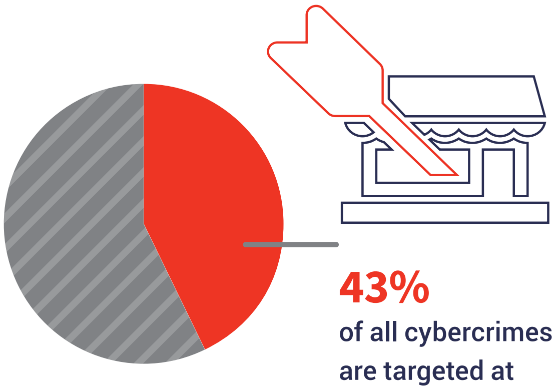
Large cyber breaches like Target, Yahoo, JP Morgan Chase or Sony have dominated the headlines. We've all read the paper and shaken our heads, asking ourselves, how could this happen? But often small businesses think that they are immune to attacks, due to their size. New data suggests that small businesses are far from immune. While the big names dominate the headlines, the reality of modern supply chains is that small businesses and large businesses work together. Each large business will have a network of small businesses providing critical services and products. In fact, small businesses are often the weakest link in the security profile of modern organisations.

The Australian Cyber Security Centre (ACSC) stated in their Threat Report that they had identified 47,000 cyber incidents over the previous financial year.

The Small Business Cyber Security Best Practice Guide published by the Australian Small Business and Family Enterprise Ombudsman notes that small business is the target of 43% of all cybercrimes. Yet an astonishing 33% of businesses with fewer than 100 employees don't take proactive measures against cyber security breaches and 87% of small businesses believe their business is safe from cyber attack because they use antivirus software alone.

Small business targets

Total 47,000 cyber incidents last financial year



43%

of all cybercrimes are targeted at small businesses

For the past 13 years, the Ponemon Institute has conducted an annual Cost of a Data Breach Study in order to measure exactly how much lost and stolen records could cost organisations around the world.

Global study at a glance

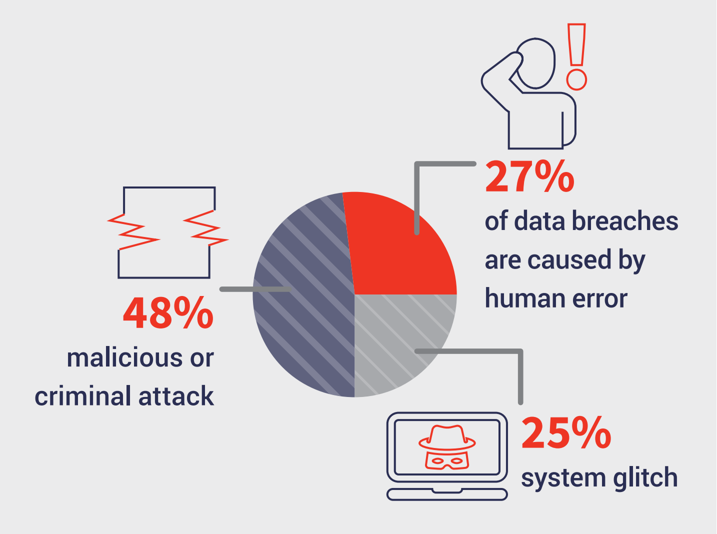
- Average total cost of a data breach in Australia: **$1.99M**
- Average total one-year cost increase: **6.4%**
- Average cost per lost or stolen record: **$148**
- One-year increase in per capita cost: **4.8%**
- Likelihood of a recurring material breach over the next two years: **27.9%**
- Average cost savings with an Incident Response team: **$14 per record**

> Here is an astonishing prediction:
>
> **According to the research firm Cybersecurity Ventures, the cost of cybercrime globally will exceed $6 trillion annually by 2021.**

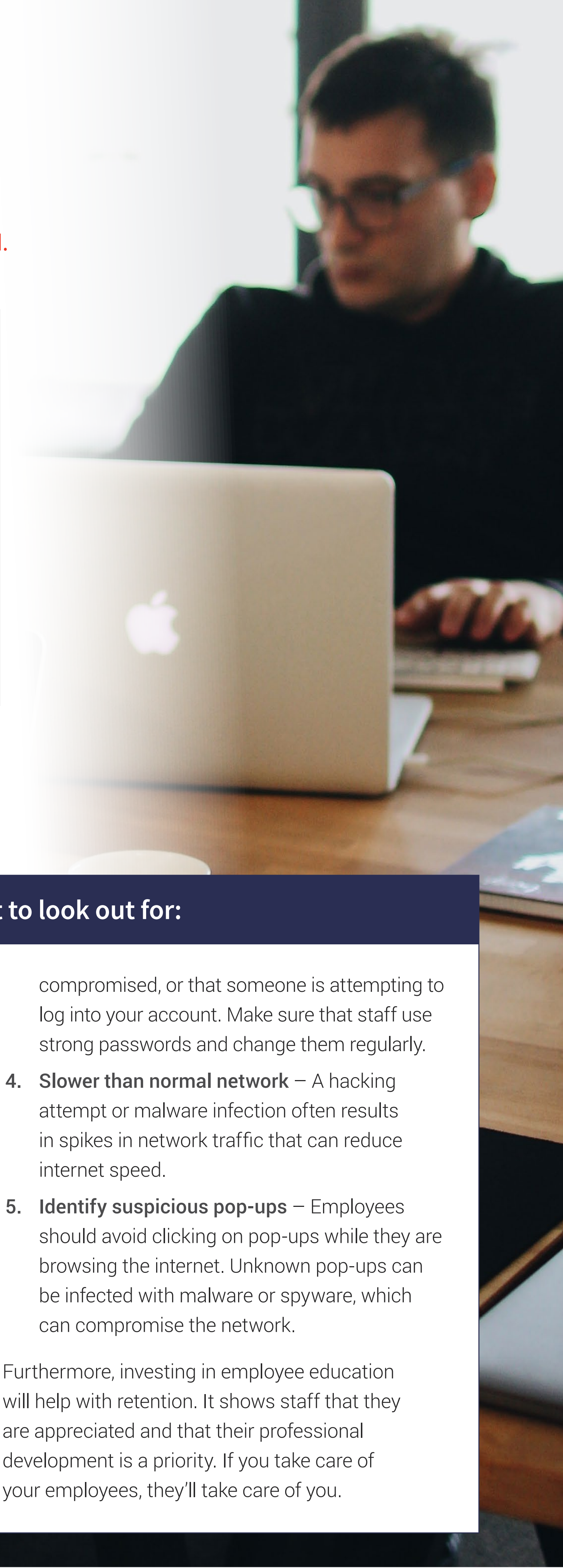
But the good news is there are multiple ways to protect your small business from cybercrime. In this report, we outline, what are in our opinion the most important measures that small businesses can do to increase their cyber resilience.

1 Education

The importance of cyber literacy cannot be underrated. 27% of data breaches are caused by human error.



Making sure that you and your staff are aware of some of the methods used by cyber criminals and things that they can do every day to help keep the business safe and secure are as important in the cyber context as having locks on your doors.



Make sure that your employees know what to look out for:

1. **Phishing** – Email phishing is one of the most common ways that hackers attempt to gain access to your network. The malicious email contains a link to an unknown source, which can unintentionally download malware onto the computer, giving hackers a window to your systems.
2. **Social engineering fraud** – It is a confidence scheme that intentionally misleads an employee into sending money or diverting a payment based on fraudulent information that is provided to the employee in a written or verbal communication such as an email, fax, letter or even a phone call.
3. **Unusual password activity** – If you're locked out of your system or you receive an email stating that a password has been changed, it is a potential sign that the password has been compromised, or that someone is attempting to log into your account. Make sure that staff use strong passwords and change them regularly.
4. **Slower than normal network** – A hacking attempt or malware infection often results in spikes in network traffic that can reduce internet speed.
5. **Identify suspicious pop-ups** – Employees should avoid clicking on pop-ups while they are browsing the internet. Unknown pop-ups can be infected with malware or spyware, which can compromise the network.

Furthermore, investing in employee education will help with retention. It shows staff that they are appreciated and that their professional development is a priority. If you take care of your employees, they'll take care of you.

2 Password protect everything

Passwords are an easy way to protect your data. They provide an immediate way in which you can secure the data contained within your network. But if the password that you use to protect one of your organisation's biggest assets is 123456, then you might want to rethink your security plan. They are your first line of defence in protecting your network and the data within it.

The UK's National Cyber Security Centre ranked the most common passwords that have been hacked. So here they are:

1.	123456	6.	12345678
2.	123456789	7.	abc123
3.	qwerty	8.	1234567
4.	password	9.	password1
5.	111111	10.	12345

Any password that can be guessed, just isn't going to cut it. Despite what all of those annoying prompts for annoying characters and upper case letters might have you believe, length matters more than complexity. Once you get into the 12-15 character range, it becomes so much harder to use any form of brute force attack to guess your password. For example, a password like F%$#0## does you way less favours than Skinnydippingnakedinchinatownpineapple1

> "Sometimes though, not even a naked skinny dip in China Town with a pineapple is enough to keep the hackers at bay."

Many of the services that you use (Facebook, Google, Outlook) already have an added layer of protection known as two factor identification available.

You might have set up your account ages ago and never have switched it on, but it's there in the application's settings and all you need to do is turn it on. Two factor identification links a back-up email or mobile number to the service. When you attempt to log into a site, the site will email or SMS you a code, which you then need to enter before you can proceed. Many organisations, such as your bank or super fund, may already require two factor identification as an additional layer of security, so you're probably familiar with the concept.

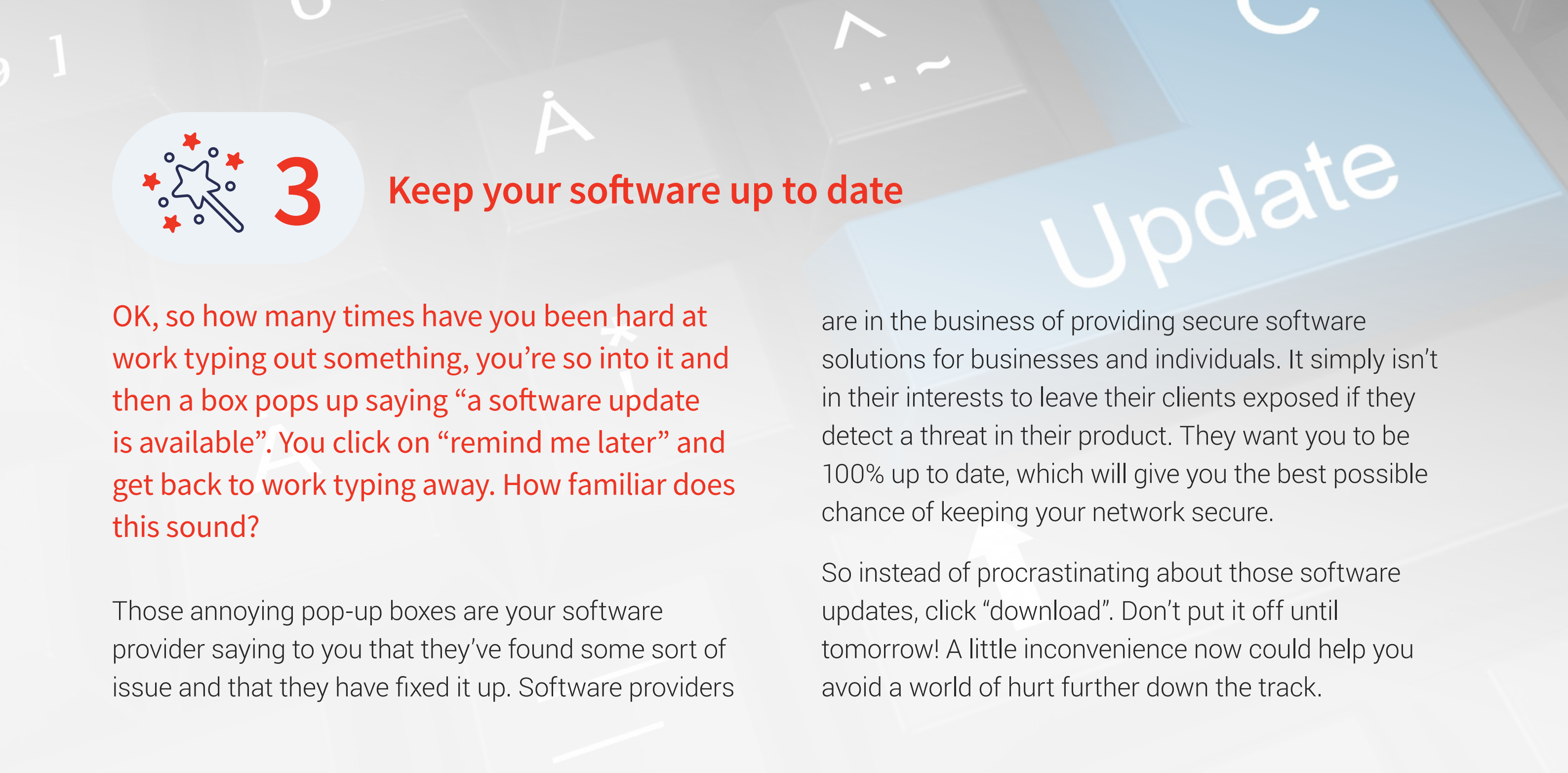
Two factor identification is just so much harder to crack than a password that can be put into a web portal from anywhere in the World, because it means that the hackers also need to have your phone number or email account. SMS is probably better to use for two factor identification than email, for the simple reason that you only have one phone number and one phone.

HACKER TECHNIQUE: Credential stuffing

As people have needed more and more passwords to log into the various systems that they use during their day to day lives, its become commonplace for people to use the same password across multiple systems. You may have come up with a doozie that you know is going to be super hard to crack but easy to remember so you start using it for everything. Your work log in, social media, email, desktop, iTunes, you name it. Maybe even that dating site that you signed up for years ago. Well if any of those sites have ever been breached, then your user name and password may have been compromised. If you used that same user name and password on another site, then you may be at risk of credential stuffing.

Credential stuffing is the process of taking user names and passwords that have been obtained through another data breach, and trying to use them to gain access to another site that you might have signed up to. Maybe you used the same password from MySpace for your bank account.

An easy way to stay one step ahead of the hackers, is to update all of your passwords at regular intervals and use different passwords for different applications, wherever possible.



3 Keep your software up to date

OK, so how many times have you been hard at work typing out something, you're so into it and then a box pops up saying "a software update is available". You click on "remind me later" and get back to work typing away. How familiar does this sound?

Those annoying pop-up boxes are your software provider saying to you that they've found some sort of issue and that they have fixed it up. Software providers are in the business of providing secure software solutions for businesses and individuals. It simply isn't in their interests to leave their clients exposed if they detect a threat in their product. They want you to be 100% up to date, which will give you the best possible chance of keeping your network secure.

So instead of procrastinating about those software updates, click "download". Don't put it off until tomorrow! A little inconvenience now could help you avoid a world of hurt further down the track.

4 Secure and Hide your Wi-Fi

Many hacking victims are compromised via Wi-Fi networks, through a technique called "wardriving." Hacker gangs drive around cities with high powered antennas, scanning for unlocked or poorly protected networks. Once a vulnerable Wi-Fi hot spot is found, the crooks are as good as in the victim's front door.

While it might sound far-fetched to think that there are actually gangs of computer criminals driving round pinching our personal information from thin air, it's actually quite common and is one of the easiest methods to gain unauthorised access to a network.

The best defence against exploits like wardriving is to have no wireless network at all. Wired networks, while less versatile, are more secure, because users have to access them by either plugging into physical outlets or hacking modem ports. But if your organisation must have a wireless network, disable the service set identifier (SSID) broadcasting function on the wireless router. This creates a cloaked or hidden network, invisible to casual Wi-Fi snoops and accessible only to users with the exact network name. Small businesses like coffee shops can also do this – just periodically change the network's information and place a small sign near the register with the current network name and passcode.

Some additional tips to help secure your wireless network include:

- **Turn off your wireless network when you're not using it:** This will minimise the chance of a hacker accessing your network.
- **Change the administrator's password on your router:** Router manufacturers usually assign a default user name and password allowing you to setup and configure the router. However, hackers often know these default logins, so it's important to change the password to something more difficult to crack.
- **Enable encryption:** You can set your router to allow access only to those users who enter the correct password. These passwords are encrypted when they are transmitted so that hackers who try to intercept your connection can't read the information.
- **Use a firewall:** Firewalls can greatly reduce the chance of outsiders penetrating your network since they monitor attempts to access your system and block communications from unapproved sources.

5 Have information security policies in place

Do you have a privacy policy? Do you have an IT security policy? Do you have a BYOD policy? Ok, so if you don’t have one, then how do your employees and external stakeholders know your view on these sorts of issues? Having a policy in place is a simple, cheap and easy way to communicate your organisation’s stated goals to your employees and stakeholders.

These policies define the who, what, and why regarding the way in which you would like your employees to act, and they play an important role in your organisation’s overall security posture. Information security policies should reflect the risk appetite of management and serve to establish an associated security mindset within your organisation.

The goal when writing an information security policy is to provide relevant direction and value to the individuals within an organisation. Make your policies brief, succinct and easy to understand. Make sure that you lead by example in following your policies. Policies become harder to enforce if management consistently flaunt them. Your staff look to management for guidance and to establish baseline culture. A “do as I say, rather than a do as I do” culture isn’t the way to get your staff to follow your policies.

The average Australian home has 17 connected devices.

80%

of all BYOD (Bring Your Own Device) is completely unmanaged in the workplace

Data source: https://www.stanfieldit.com/cyber-security/

6 Back up your data

Your business data is one of the most valuable assets of your business. Therefore, it’s important to make sure you store your data (including financial, registration and customer records) and other important business documents in a safe location and that data is backed up.

For small businesses, backing up data doesn’t mean that you need to replicate offsite servers, or use tapes to download data. There are a range of cloud based backup services that can be used. They vary in price and the features that they offer.

Cloud backup services for businesses work by providing customers with access to shared, virtual storage infrastructure. This lets providers create a large pool of data storage, parcel it out among its customers, and manage the whole thing down to the byte level.

PC Magazine recently published an article titled The Best Cloud Backup Services for Businesses for 2019 where they compared a number of popular Cloud based backup services. Many more cloud based back up services are available.

By backing up your data, you’re able to restore your systems in the event that a cyber incident occurs.

7 Have a business continuity plan

A Business Continuity Plan (BCP) involves making a plan for how your business can prepare for and continue to operate after an incident or crisis. This could be any sort of incident, and doesn't necessarily have to be a cyber incident.
An element of the BCP can include a Data Recovery Plan (DRP). A DRP is your plan for how you're going to recovery your data following a system outage.

> A business continuity plan will help you to:
>
> - identify and reduce risks where possible
> - prepare your business for risks that you can't control
> - respond and recover if an incident or crisis occurs.

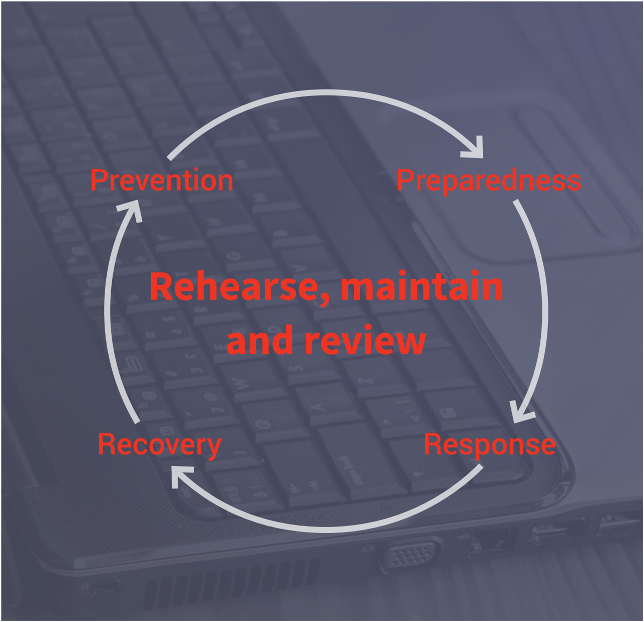
Many small businesses owners might be thinking "Great! Another time consuming task that's going to take me away from revenue producing activities!" In actual fact, a well prepared BCP might help you attract new business by using the BCP to appeal to customers and let them know that you have robust procedures in place to continue to provide them with services in the event of a disaster. A BCP can even help you to attract investment. Most venture capitalists, private equity firms, hedge fund managers or angel investors will require a BCP be in place before they agree to invest money into a company. It's only natural that they would want to make sure that any funds that they put into an enterprise are in safe hands in the event that the unthinkable occurs.

By going through the exercise of preparing a BCP you'll be much better prepared to deal with the minor mishaps in life as and when they occur, which they inevitably will. You'll better understand your supply chain and the strengths and weaknesses of your organisation.

But just having a BCP is one thing, you also need to regularly test your BCP to make sure that it will work in the event of a crisis. One way to do this is to role play it with your staff. Create a fake scenario that effects your business. It doesn't have to be a cyber attack. It could be anything, from an earthquake to a terrorist attack. Employees go through the motions as if the event has occurred and you then follow the BCP measuring how long it takes to get your organisation back up and running. How long did it take? How much working capital do you keep aside? Do you have enough cash to meet your cash flow requirements? Do your employees all know what their roles are? Do you know how to recover your data? How were you communicating with your team during the crisis?

After the business continuity plan is put to the test, gather your employees to discuss the plan's overall performance. Identify where it needs improvement and the parts that worked best. Make changes to key persons and actions where necessary, to ensure that the BCP is working at its best. Having a business continuity plan is good, but testing it regularly is equally important.

If you're looking for a free template to use, the Queensland Government has published a BCP template, which is available for download



8 Make sure that you have adequate insurance

A robust risk management framework is essential, but isn't necessarily going to completely protect your organisation from the devastating fallout of a cyber attack. We have locks, CCTV cameras, security systems and sprinkler systems at our premises, but still buy property insurance right. Buying cyber insurance is no different.

Many organisations continue to self-insure their cyber risk. When you think about the average cost of responding to a cyber incident, this would be enough to put most small businesses out of business. Yet cyber insurance is one of the least purchased insurance products available.

Insurers have developed cyber liability insurance policies that are specifically designed to cover the unique risks associated with a cyber or privacy incident.

Insurers will generally ask questions about your organisation's controls before they'll accept your cyber risk. Insurers will want to know that you're doing what you can to mitigate your cyber risk before they agree to transfer that risk to their own balance sheets. So before you go and get a quote, make sure that you've got the basic risk management procedures in place.

Not all policies are the same though and it pays to properly read the policy wording so that you thoroughly understand the cover that you're buying. Unlike the property or general liability markets, which have been insuring the same risks for centuries, the cyber market is in its infancy and the risks themselves are still developing. The cover available in some policies in the market differs significantly.

Cyber coverage generally includes:

- Privacy breach notification costs
- Business interruption loss
- Incident response
- Cyber extortion costs
- Forensic support
- Legal support

Talk to your insurance broker today about insuring your organisation's cyber risk. Your broker will be able advise you of the various products available in the market and guide you towards one which suits your individual risks and budget.

About the co-authors

Jaydon Burke-Douglas is a qualified solicitor and insurance professional. He is admitted to practice law in New South Wales and the Commonwealth. He has held a variety of roles at some of the World's largest insurers and underwriting agencies. He has a passion for helping small businesses understand their cyber exposures and implement strategies to assist them in mitigating their cyber risk.

Hamish was appointed as Executive Director of ProRisk and Armada in August 2017. He is responsible for developing and implementing ProRisk's business strategies and managing a diverse underwriting portfolio of Financial Institutions, General Liability, Property, Motor, Accident and Health and Speciality Consumer Products.

Hamish has had an extensive career in insurance underwriting and broking across Corporate, SME and Scheme business. Hamish is a specialist in financial lines insurance and experienced in the development of rating models, product development, wording drafting, portfolio analysis, business development and strategy, and professional development and training.

☎ 03 9235 5255 ✉ enquiries@prorisk.com.au www.prorisk.com.au

Disclaimer: The information and advice contained within this paper is general in nature intended only as a guide. It is does not take into consideration your organisation's specific cyber security needs and is not an exhaustive list of all of the possible methods that you can employ to protect your organisation from a cyber attack. It is intended to be used as an educational tool and we encourage you to seek professional advice to properly assess your risk of a cyber attack. We do not warrant any of the information contained in any links to third party websites contained in this paper.