BizCover for Brokers

Broking Streamlined.

Cyber Threats Explained

A guide for small businesses

Including how AI is changing cyber risk



Cyberattacks aren't just a problem for big businesses.

From fake invoices and phishing emails to stolen passwords and ransomware, small businesses face cyber threats every day. And if one hits your business, the consequences could go far beyond lost money.

The good news: Understanding the risks can help you prepare. This guide breaks down common cyber threats facing Australian small businesses, how they happen, how AI is changing risk, and practical steps you can take to help protect your business.

A suspicious email, a dodgy link, a simple mistake... Cyber threats can take many forms. Here are some of the most common that your small business may experience.

INSIDE THIS GUIDE

What a cyber incident can cost 03

COMMON CYBER THREATS

Someone tricks you or your people 04

Someone locks your systems 05

Someone steals your money 06

Someone steals or exposes your data 07

A person, process, or technology control fails 08

Someone pretends to be you or takes over your account 09

A supplier or service provider is hit with a cyberattack 10

PROTECTING YOUR BUSINESS

Five common myths 11

Cyber Insurance: your safety net 12

Cyber self-check 13



THE REAL COST

The cost of cyber incidents for small businesses



Money

$55,400

The average self-reported cost of cybercrime for small businesses was $55,400 in FY2026[1].

What might go into this number? Fraudulent payments, ransomware extortion paid in the initial attack, and lost revenue from trading interruptions. Then there are the costs associated with getting back to business: incident investigation, recovery services, customer notification, and legal or regulatory advice.



Time

Systems disabled or locked out of essential accounts? That's precious time and productivity lost.

But everything that comes after a cyber incident—restoring systems, contacting your bank, meeting with solicitors, and notifying affected clients and suppliers—also take time away from serving customers and running your business.



Reputational harm

Cyber incidents can impact how your clients, customers, suppliers, and partners feel about your business.

Missed orders, service outages, corrupted files, and stolen data are just some of the outcomes from a cyberattack or breach. Any one of these could make people think twice about working with your business in the future.

1. ASD, Annual Cyber Threat Report 2025-2026

THREAT 1 OF 7

Someone tricks you or your people

> How do you verify urgent requests before anyone shares information or moves money?

SCENARIO

You receive a call from a partner asking for documents connected to some mutual clients. They say the matter is urgent and email you a link to a file sharing service where you can upload the requested docs. You do it, only to later discover that the call was a fake. You've shared confidential client information with a cybercriminal.

ALSO KNOWN AS...

Social engineering, phishing

27%

of small businesses surveyed received an email pretending to be from a trusted supplier, bank, or government agency in FY26[1].

HOW IT HAPPENS

Fraudulent requests for payment or information may arrive by email, SMS, phone, video meeting, or social media. They may use a lookalike email address or spoofed phone number to appear legit. Others rely on hacking into accounts belonging to trusted partners, like your suppliers, bank, or employees.

The request is typically urgent, hoping you'll act fast without verifying the details.

HOW AI AMPLIFIES IT

AI can create polished messages and imitate tone of voice. It also makes it faster and easier for criminals to gather information about you and your partners, so they know just what to ask for.

ACTION STEPS FOR SMALL BUSINESSES

- Call the sender to confirm requests (even urgent ones) using a known phone number, not details provided in the message, phone call, or meeting.
- Restrict who within your business is permitted to share information, reset passwords, or change account details.



1. BizCover survey of 545 Australian small business owners, conducted by Antenna, July 2026

THREAT 2 OF 7

Someone locks your systems

> What programs or systems would stop your business from trading if they were unavailable for hours or days?

SCENARIO

You receive an email from a partner with an attachment. You download it, only to find yourself completely locked out of your computer. You can't access any of the apps or files you need to do business.

ALSO KNOWN AS...

Ransomware, malware, remote access scams

6%

of small businesses surveyed accidentally clicked a link or downloaded an attachment that seemed legitimate in FY26[1].

HOW IT HAPPENS

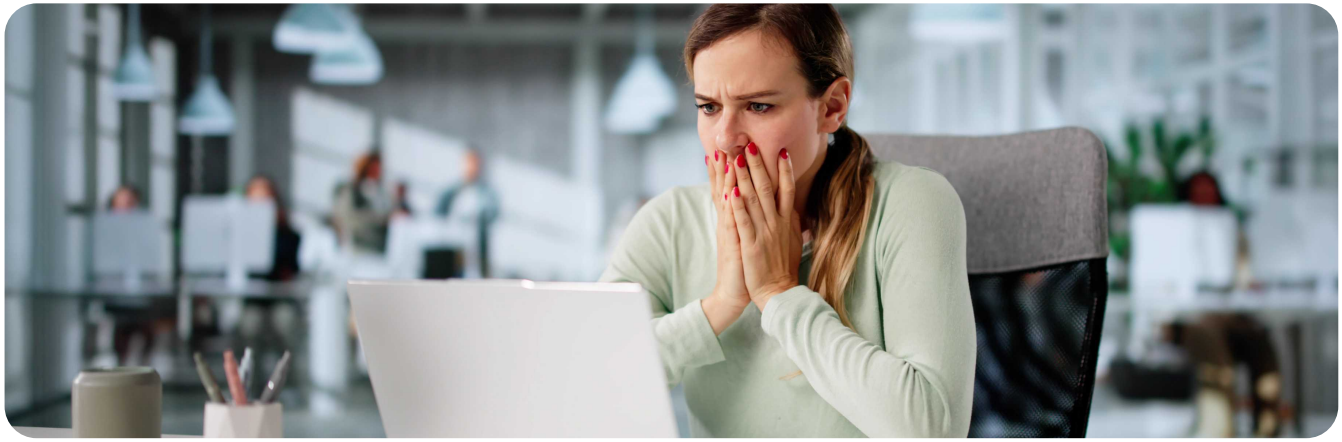
There are several methods used in these types of attacks: Malware (e.g., ransomware or malicious attachments), remote access (e.g., someone steals or tricks you into sharing your login details), unpatched software, or a service provider is involved in their own cyber incident.

HOW AI AMPLIFIES IT

AI can help make these attacks more efficient by tailoring messages and identifying likely points of entry faster.

ACTION STEPS FOR SMALL BUSINESSES

- Use multi-factor authentication (MFA) or a passkey wherever possible
- Regularly back up your data, and test how long it takes to restore systems, so you know how long you're likely to be offline if an attack occurs.
- Complete software/app updates as soon as possible to avoid leaving a door open to hackers.



1. BizCover survey of 545 Australian small business owners, conducted by Antenna, July 2026

THREAT 3 OF 7

Someone steals your money

> What happens when a regular supplier emails you with new bank details?

SCENARIO

A supplier emails to let you know that they've updated their payment details. They ask you to use this new account to pay an upcoming invoice. You do, only to later discover that you've made payment to a fraudulent account. The 'supplier' email was a clever fake.

ALSO KNOWN AS...

False billing scam, payment redirection scam

7%

of small businesses surveyed received an urgent request to change payment details from an unknown or suspicious contact in FY26[1].

HOW IT HAPPENS

A criminal can impersonate someone you trust by compromising an email mailbox, registering a lookalike domain, altering an invoice, or intercepting a text thread.

The request is often time-sensitive, with urgent consequences (e.g., "pay now or we'll cancel your contract").

HOW AI AMPLIFIES IT

AI can create polished messages and imitate tone of voice. It can create convincing invoices that use real business details, like logos and ABNs.

ACTION STEPS FOR SMALL BUSINESSES

- Call the sender to confirm requests (even urgent ones) using a known phone number, not details provided in the message, phone call, or meeting.
- Match every incoming invoice against actual purchase orders and delivery receipts.
- Restrict who within your business is permitted to approve and make payments.
- Notify your bank as soon as possible if you suspect a fraudulent payment has occurred.

1. BizCover survey of 545 Australian small business owners, conducted by Antenna, July 2026

THREAT 4 OF 7

Someone steals or exposes your data

> What information would be the hardest to explain losing control of?

SCENARIO

You receive an email asking you to log in to your cloud storage account to verify information. Turns out, the login prompt was a fake. You unknowingly gave cybercriminals your real login details, which gave them access to your customers' names, email addresses, payment details, and more.

ALSO KNOWN AS...

Data breach, phishing

HOW IT HAPPENS

Data can be stolen or exposed through stolen credentials or through a supplier who has been attacked. Lost devices, misdirected files, and incorrectly shared links can also lead to a data breach.

Your notification obligations

If your business is covered by the Privacy Act 1988 and a breach is likely to cause serious harm to the people affected (an "eligible data breach"), you'll need to take steps such as:

1. Containing the incident to stop further data theft
2. Assessing the damage to determine if personal data was stolen or exposed
3. Notify the Office of Australian Information Commissioner (OAIC)
4. Notify affected customers and/or employees

Report the cybercrime to the Australian Cyber Security Centre.

Visit the OAIC website to learn more about which businesses are covered by the Privacy Act and their reporting obligations.

HOW AI AMPLIFIES IT

AI can quickly sort stolen information, speeding up targeted scams before you even realise a theft has occurred. Data can also be exposed when sensitive information is entered into an unapproved AI service.

ACTION STEPS FOR SMALL BUSINESSES

- Use multi-factor authentication (MFA) or a passkey wherever possible
- Keep only the information you absolutely need to run your business. Create a process for reviewing and deleting old data.
- Create rules for what types of data is stored in cloud tools or shared with AI.



THREAT 5 OF 7

A person, process, or technology control fails

ALSO KNOWN AS...

Human error

32%

of cyber incidents reported to the OAIC in 2025 were caused by human error.[1]

HOW IT HAPPENS

Not every cyber incident starts with an outside attack. Misdirected emails, wrong permissions, and lost devices can lead to data breaches. Shared accounts, weak passwords, and bypassing cyber security systems are also common culprits. Usually, a combination of human mistakes, breakdown of processes, and technology mishaps are to blame.

HOW AI AMPLIFIES IT

Automation can make an error travel faster. Sensitive information may be disclosed through an AI tool, or unchecked AI recommendations could be used to make incorrect customer or professional decisions.

ACTION STEPS FOR SMALL BUSINESSES

- Create processes for checking emails, files, and data before they are shared. More importantly, use them every time to help avoid mistakes.
- Set up individual accounts for each staff member for commonly used software and apps. Use permissions to ensure sensitive information is only accessed by the appropriate employees.
- Use encryption and password protect files that are being shared whenever possible.

> Which routine tasks could expose information or stop work if a step is missed?

SCENARIO

A customer emails asking for an update on their order. You confirm their identity but accidentally attach the wrong invoice in your reply. The document you shared contained payment details for another customer.

1. OAIC Notifiable Breaches, Jan-Jun 2025 and Jul-Dec 2025

THREAT 6 OF 7

Someone pretends to be you or takes over your account

> How quickly would you know if a client received a fake invoice or message from your business?

SCENARIO

A cybercriminal hacks into your email and social media. They start sending a fake offer to customers and ask them to pay deposits into their account. You're locked out, and your customers are not happy.

ALSO KNOWN AS...

Account takeover, business impersonation, business email compromise (BEC)

4%

of small businesses surveyed had a business email, website, or social media account compromised, locked, or taken over in FY26[1].

HOW IT HAPPENS

Reused passwords, stolen login credentials, and malware can all lead to a takeover. However, criminals sometimes create a fake website or social media accounts using lookalike URLs to impersonate real businesses.

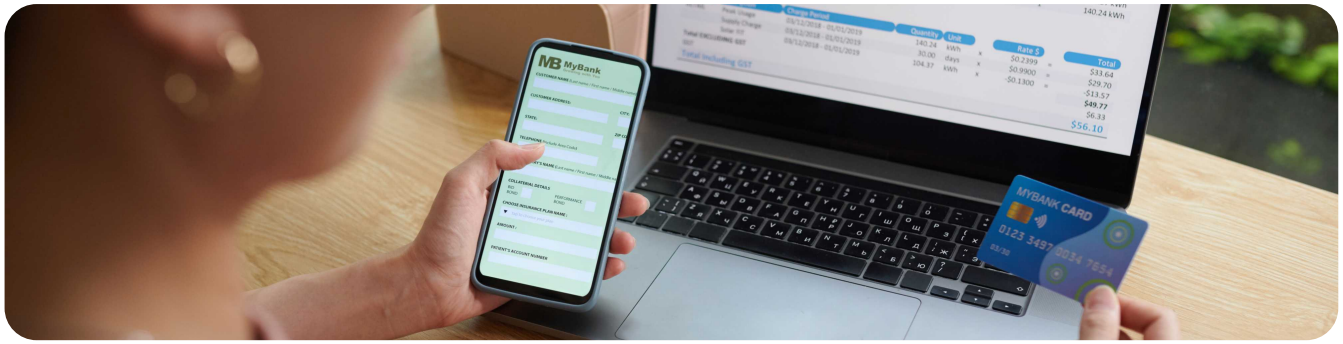
Regardless of how it happens, the fallout for your business is the same: Customers, clients, and suppliers may lose trust in your business. They may doubt real communications you send in the future or simply move on to a competitor.

HOW AI AMPLIFIES IT

AI can reproduce your business' tone, branding, and public content to create convincing emails, messages, audio, and video.

ACTION STEPS FOR SMALL BUSINESSES

- Use multi-factor authentication (MFA) or passkey wherever possible
- Use unique passwords and passkeys
- Keep an eye on suspicious emails and messages, customer complaints, and changes to your website or social media accounts.
- Have customer messages and a response process ready to go should an incident occur.



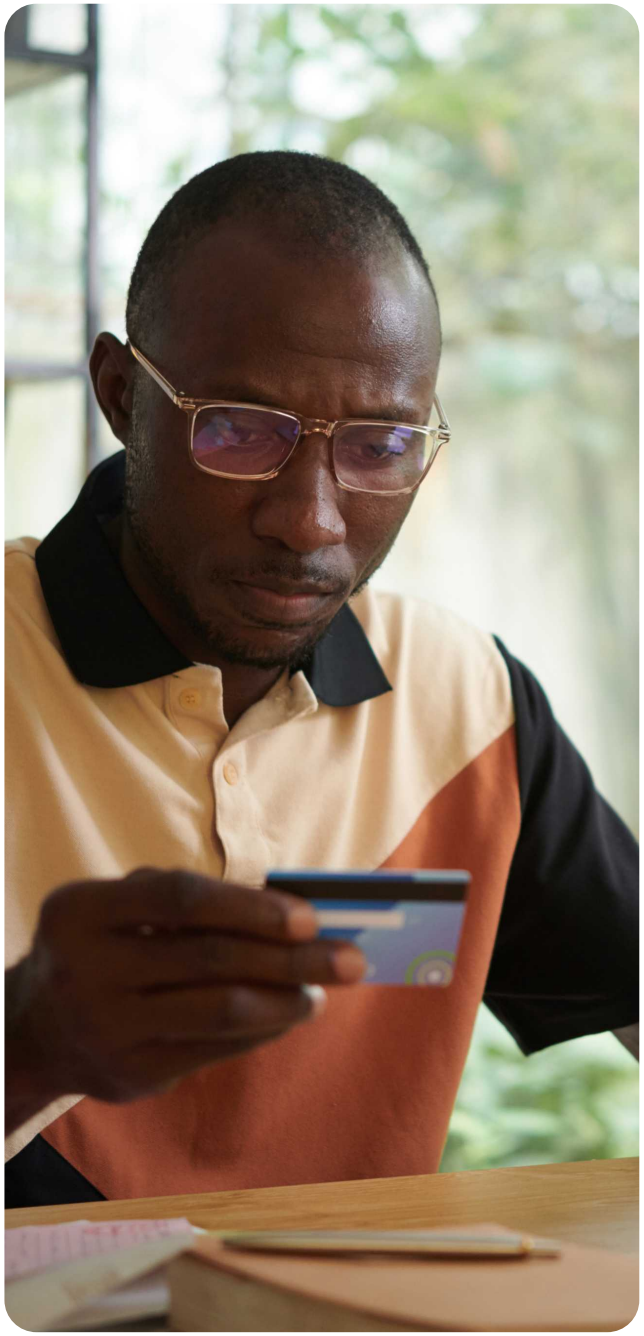
1. BizCover survey of 545 Australian small business owners, conducted by Antenna, July 2026

THREAT 7 OF 7

A supplier or service provider is hit with a cyberattack

HOW IT HAPPENS

The service providers and suppliers you work with can experience the same cybersecurity scenarios as you: social engineering, phishing, scams, business email compromise, and more. And when they go down, they may take you and other small businesses with them.



> Could an attack on those you work with stop your business from trading or expose your data?

SCENARIO

Your third-party payment service suffers a cyberattack that causes a software outage. You're unable to process payments for several hours until the issue is resolved. To make matters worse, the attack also exposes your customers' payment data.

ACTION STEPS FOR SMALL BUSINESSES

- List critical suppliers and service providers, as well as the data they may have access to.
- Understand what a service provider's responsibilities are to you, such as incident notification, data return, and support to affected customers.
- Outline steps for keeping your business running if a critical piece of software or app stops working.

MYTH VS REALITY

Do I really need to worry about all this?

Cyberattacks are a bigger problem for small businesses than you may realise. Let's break down five common myths we hear from business owners every day:

MYTH 1

"We're too small to be a target."

43% of small businesses surveyed experienced a cyber incident in FY26[1].

Small businesses are easy targets for cybercriminals. They're typically less protected than larger businesses, both because they may not realise the risk and because they don't have as much money to put towards cybersecurity.

MYTH 2

"Our IT provider takes care of cyber stuff."

Your provider may manage technology, but your business controls payments, system access, data decisions, and communication. These provide plenty of entry points for cybercriminals.

MYTH 3

"Everything is stored in the cloud."

Cloud storage can improve resilience, but it doesn't remove cyber risk. Data on the cloud is not always be secure. For example: cybercriminals may be able to access cloud-based data with stolen login details.

There's also human error and tech issues to consider. Depending on the service and settings, data stored in the cloud can be accidentally deleted or corrupted.

MYTH 4

"We don't hold sensitive information."

Are you sure? Bank details, staff records, business contacts, contracts, and login details are all enticing to thieves.

Some cyber risks have nothing to do with stealing information. Disrupting your business operations, impersonating your business, and soliciting fraudulent payment are also common cyberattack goals.

MYTH 5

"We have backups, so we're covered."

Backups are only useful when they are complete, stored securely, and tested. Plus, they don't recover fraudulent payments or replace lost trading time.

1. BizCover survey of 545 Australian small business owners, conducted by Antenna, July 2026

CYBER INSURANCE

Cyber Insurance: Your Business' Safety Net

You've studied the risks and taken steps to protect your business systems. Great! Unfortunately, cybercriminals are good at staying one step ahead of technology, slipping through defences, and creating believable scams.

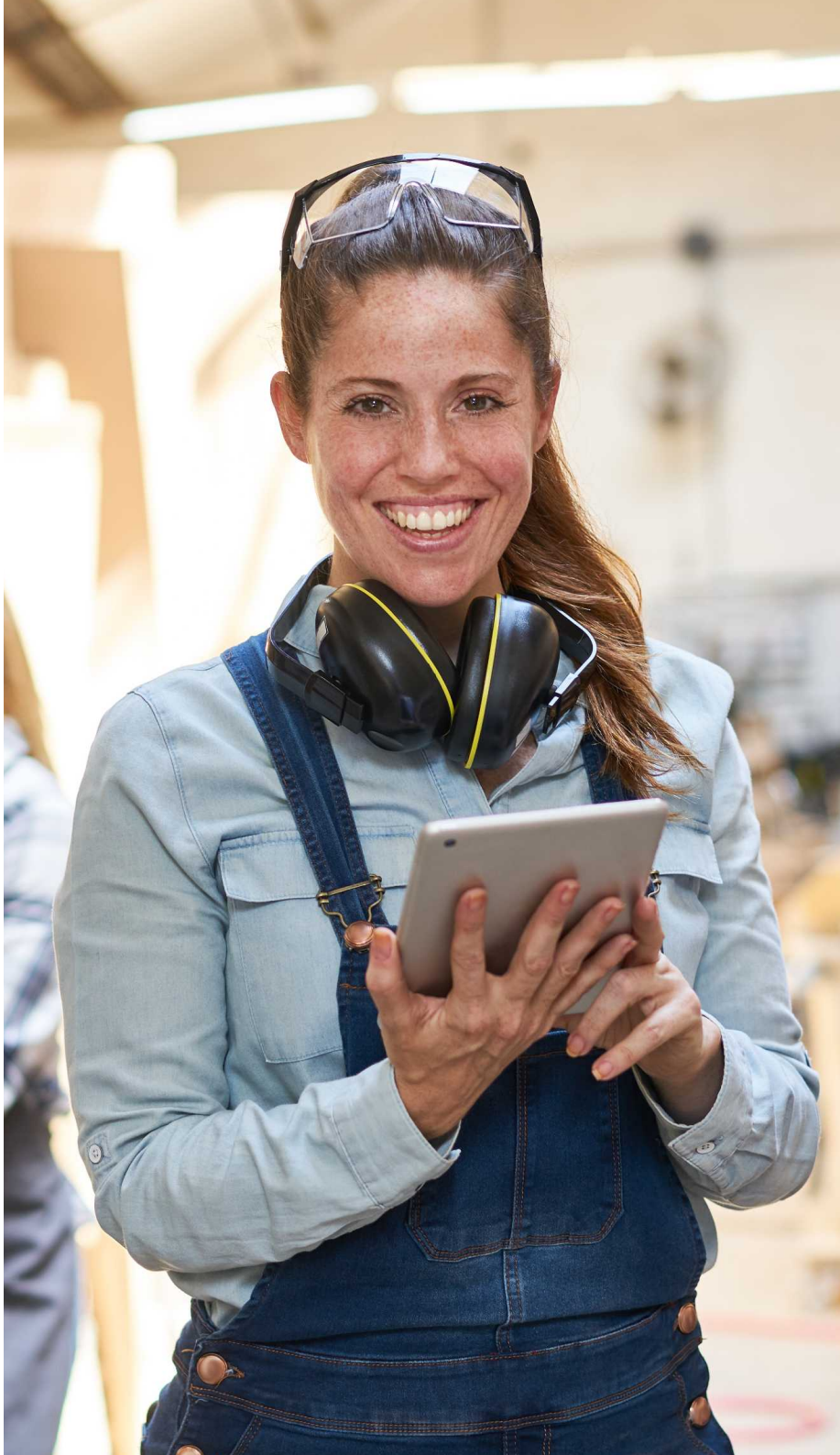
That's when you may want a safety net to help you get back to business following a cyberattack or data breach.

Cyber Insurance can help you manage many types of cybercrime (like cyberattacks, ransomware, and data breaches) by covering legal costs, data recovery, fines and penalties, and other expenses related to the cyber event. You can also add optional cover for Social Engineering, Phishing or Cyber Fraud.

A Cyber policy can do more than just protect your savings and cash flow. It can also connect you with IT support during or after an attack.

Many Cyber policies include access to a 24/7 incident response hotline just for policyholders. This service can connect you with resources and support to help minimise the damage and get you back to business as usual, as quickly as possible.

Interested in Cyber Insurance for your small business? Contact your broker to learn more.



CYBER SELF-CHECK

How cyber-safe is your business?

This checklist can help you discover where you're doing well and areas that may need some improvement. It's a good place to start, especially if you're thinking about cybersecurity for the first time.

Mark each item as Yes, Needs checking, or Not yet.

	QUESTION	YES	NEEDS CHECKING	NOT YET
1	Do we know which systems we need to keep the business running?	☐	☐	☐
2	Do we independently verify changes to customer or supplier bank details?	☐	☐	☐
3	Do important payments require approval from a second person?	☐	☐	☐
4	Do we use multi-factor authentication (MFA) or passkeys on important accounts and systems?	☐	☐	☐
5	Does everyone have their own account, with admin access limited to only those who need it?	☐	☐	☐
6	Do we regularly back up important data and test that we can restore it?	☐	☐	☐
7	Are our devices and software kept supported and up to date?	☐	☐	☐
8	Do we regularly check our systems for security weaknesses and fix serious issues promptly?	☐	☐	☐
9	Do we know what sensitive information we hold and where it is stored?	☐	☐	☐
10	Do we have clear rules for using AI tools, including what information can and cannot be entered into them?	☐	☐	☐
11	Do we remove information and user access when they are no longer needed?	☐	☐	☐
12	Do we know which suppliers and technology providers are critical to our business?	☐	☐	☐
13	Do we regularly train our people to recognise phishing, scams, and suspicious requests?	☐	☐	☐
14	Does everyone know how and where to report something suspicious or a possible cyber incident?	☐	☐	☐
15	Do we have an incident response plan, key contacts, and someone responsible for leading the response?	☐	☐	☐
16	Could we continue operating if our email or key systems were unavailable for several days?	☐	☐	☐
17	Do we have a Cyber Insurance policy, and do we know who to contact if an incident occurs?	☐	☐	☐

BizCover for Brokers

Broking Streamlined.

BizCover for Brokers acts as agent of the insurer and not as the agent of you or your client. This information is general advice only and does not take into account your objectives, financial situation or needs. It should not be relied upon as personal advice. As with any insurance, cover will be subject to the terms, conditions and exclusions contained in the policy wording or Product Disclosure Statement (available on our website). Please consider whether the advice is suitable for you before proceeding with any purchase. Target Market Determination document is also available (as applicable).

© Copyright 2026 BizCover Pty Limited. BizCover for Brokers is a business name of BizCover Pty Ltd (ABN 68 127 707 975; AFSL 501769). BC4000 MRFA-8221