BizCover for Brokers
Broking Streamlined.

Cyber Threats Unveiled

How Cyber Liability Insurance may respond in the event of an incident and help protect your clients

BizCover for Brokers
Broking Streamlined.

Cyber threats are everywhere...

And they often target small and medium businesses across Australia. In 2022, the average cost per cybercrime increased to over $39,000 for small businesses.[1]

With 43% of cyberattacks targeting SME businesses and only 5% of their data folders protected, it may only be a matter of time before your clients suffer one too.[2]

This pocket guide can help you discuss potential cyber threats with your clients and illustrate the importance of Cyber Liability & Privacy Protection insurance.

MALWARE

What is it?

Malware is any malicious software that can be installed on your computer or other devices (such as a mobile phone or tablet). Common types of malware include:

Viruses

Spyware

Ransomware

Trojan horses

Keystroke loggers

Email is the most common way that malware is delivered to devices. It can appear to be from a legitimate source, such as a government agency, utility provider, or the police. Your clients' employees may also receive emails that appear to be from their employer that are really malware scams. Clicking on a single link is often all it takes to unknowingly download malware to a device.

Let's take a closer look at some common cyberattacks using malware that your small business clients might encounter.

1. ACSC, **Annual Cyber Threat Report**, July 2021 to June 2022
2. MyBusiness, **Almost Half of Australian Cyberattacks Hit SMEs**, April 2022

BizCover for Brokers
Broking Streamlined.

REMOTE ACCESS SCAMS
What are they?

Remote access scams usually begin with a phone call claiming that your computer is infected with a virus or another fake but credible story requiring access to your computer. You're asked to follow instructions to allow the caller to access and control your computer to fix the problem. Instead, the caller steals your information or installs a Trojan horse or other type of malware. They might also try to get you to purchase 'anti-virus' software, which is usually overpriced or freely available on the internet.

EXAMPLE

Cybercriminals impersonated the Insured's bank over the phone and advised they were doing an audit and needed to verify some recent transactions. The Insured confirmed their log in details and security code to authenticate log in.
The cybercriminals used this information to transfer around $80,000 out of the Insured's account.

POLICY RESPONSE

Cover was available for IT forensics to confirm no ongoing unauthorised access was occurring. The bank was able to recover around $34,000 of the fraudulent transfers and cover was available for the remaining ~$46,000.

$21.7m

REPORTED LOSSES

In 2022, remote access scams were the fifth most common scam reported in Australia. There were 11,792 of these incidents reported to the ACCC, resulting in over $21.7 million in reported losses.[3]

3. ACCC Scam Statistics, 2022.

BizCover for Brokers
Broking Streamlined.

KEYSTROKE LOGGERS & SPYWARE

What are they?

Keystroke loggers and spyware record everything you type on your keyboard, allowing cybercriminals to learn your passwords and bank details or access other personal information. Once installed, they can control your email and social media accounts and may use them to send more scams to your colleagues, family or friends.

EXAMPLE

Breaches caused by keystroke loggers, spyware, and compromised passwords often occur on systems that are not using Multi-Factor Authentication (MFA).

Cybercriminals often use login information to gain access to a business' email. Once inside, they can easily steal sensitive data or carry out social engineering scams to target the business' clients, vendors, or suppliers.

POLICY RESPONSE

Policies may respond to malware or unauthorised access to an Insured's network. IT forensic firms can assist the Insured by:

- Securing their systems
- Identifying what actions were taken by cybercriminals
- Recommending steps to prevent future attacks

Cover is also available for legal fees in obtaining advice on the Insured's obligations under the Privacy Act, as well as under some contracts with clients if their data is compromised. One of our Insurer partners revealed that the average costs for these types of incidents are approaching $100,000.

BizCover for Brokers
Broking Streamlined.

RANSOMWARE
What is it?

Cybercriminals install ransomware to encrypt or lock your device, forcing you to pay a ransom to unlock it. However, paying doesn't guarantee that it will be unlocked. Your unlocked device could also have hidden viruses, which spread and infect other computers and devices on your network.

$1,172,000 REPORTED LOSSES

The ACCC received 3,623 reports of ransomware and malware in 2021, with reported losses of over $1,172,000.[4]

4. ACCC **Scam Statistics**, Ransomware & malware, 2021.

EXAMPLE

A manufacturing company's network of 20 computers was affected by ransomware, with users unable to access files, which had been encrypted. The ransomware entered the computer network via an infected email attachment which had been inadvertently opened by an employee. A message appeared on the employee's screen demanding a ransom be paid in exchange for the code to unlock the encrypted data.

The insured's external IT provider was able to re-build and recover the server and rebuild lost data from back-up.

POLICY RESPONSE

The ransomware was removed, the data was recovered from back-up and the insured did not pay the ransom. There was no actual or suspected loss of data but there were costs involved in containing and recovering from the incident.

The external IT costs included work to verify the issue, removal of the malware, checking PCs manually for corrupted files, downloading backups and getting software back for users. Costs were reviewed and accepted by the Insurer and they were paid under the policy.

SOCIAL ENGINEERING

What is it?

Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker. All techniques aimed at convincing a target into revealing specific information or performing a specific action for illegitimate reasons.

Now let's explore common ways that social engineering happens.

BizCover for Brokers
Broking Streamlined.

$24.6m
REPORTED LOSSES

Phishing was the number one reported scam in Australia in 2022. The ACCC received 74,576 reports that resulted in losses totalling over $24.6 million.[3]

3. ACCC **Scam Statistics**, 2022.

PHISHING

What is it?

Phishing is when cybercriminals send fake emails, SMS, or messages via social media pretending to be a trustworthy business or individual. The message may ask you to click on a link, enter your login details, or transfer money. Typically, phishing messages create a false sense of urgency to trick someone into taking action without questioning the source.

EXAMPLE

There are typically two types of Phishing attacks, internal and external:

External – The Insured receives a message from cybercriminals pretending to be someone they trust. They convince the Insured to download a file or click on a link which downloads malware or causes the Insured to reveal their login details.

Internal – The Insured's systems are compromised by an external phishing attempt. Cybercriminals then use the business' email to convince employees to give up sensitive information or transfer money. They may also forward phishing attempts to the Insured's clients.

POLICY RESPONSE

Policies typically respond to unauthorised access and IT forensics are appointed to assist the Insured in understanding the full scope of the breach.

Legal Fees would also be covered if access to sensitive information is confirmed. If an optional extension for social engineering is purchased, cover is typically available for the social engineering payments.

Costs can vary significantly depending on the scope of the breach. One of our insurer partners reported they are seeing costs usually between $25,000 and $75,000, but in some cases exceeding $150,000.

BizCover for Brokers
Broking Streamlined.

FALSE BILLING SCAMS

What are they?

As the name implies, false billing scams use fake invoices to trick businesses into paying for unwanted products or services. A common version of this is the business directory scam, where you receive an invoice supposedly from a well-known directory. You may also be tricked into signing up for a 'free' service with hidden fees or subscriptions in the fine print. These scams can be hard to spot because cybercriminals will often use the supplier's logos and branding to make them look legitimate.

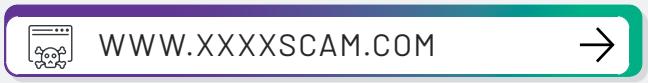
$25.3m
REPORTED LOSSES

False billing scams were the second most reported incident in 2022, with over $25.3 million in reported losses.[3]

3. ACCC **Scam Statistics**, 2022.

DOMAIN NAME SCAM

What is it?



Cybercriminals use domain name scams to trick businesses into signing up for unsolicited subscriptions or paying fake renewal invoices. You might be emailed a registration request for a domain that is very similar to your own or sent a fake domain renewal invoice for your real domain name. Scammers hope that you'll sign up or pay before you realise what's going on.

BizCover for Brokers
Broking Streamlined.

PAYMENT REDIRECTION SCAMS

What are they?

Payment redirection scams use information obtained through hacking, malware, or phishing—particularly the names of suppliers you work with. A scammer pretends to be one of your regular suppliers and contacts you to advise that their banking details have changed. They give you their new bank account details and ask that you use them for future payments. These scams can be hard to spot because cybercriminals will often use the supplier's logos and branding to make them look legitimate. You may not realise you've been tricked until the real supplier asks why they haven't been paid.

BizCover for Brokers
Broking Streamlined.

OTHER CYBER THREATS

What are they?

A scammer doesn't need to install malware on a device to defraud a small business.

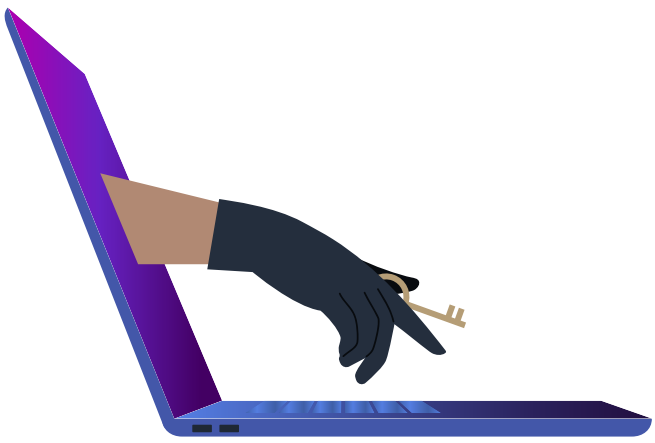
Let's look at other common cyber threats to small businesses.

DATA BREACHES

What are they?

Data breaches occur when sensitive business or customer information is lost, accessed or disclosed without authorisation. These events can be very serious for your SME clients.

Under the Notifiable Data Breaches scheme, people must be told if their details have been part of a breach that is likely to cause them serious harm.

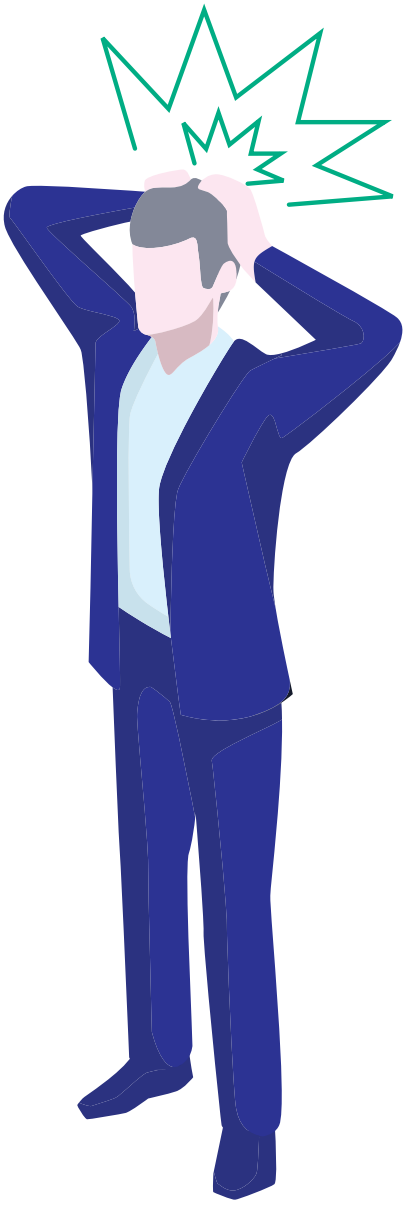


BizCover for Brokers
Broking Streamlined.

HUMAN ERROR

What is it?

Not all data breaches are caused by an outside attack or hack. A simple mistake could cause sensitive business or customer information to fall into the wrong hands. Emailing personal info to the wrong person, accidentally releasing or publishing sensitive information, and forgetting to blind carbon copy (BCC) group emails are all common ways this happens.



254
REPORTS IN 2022

Human error is the second largest cause of data breaches in Australia, accounting for 28% of total incidents reported under the Notifiable Breaches scheme in 2022.[5]

5. OAIC Notifiable Breaches, Jan-Jun 2022 and Jul-Dec 2022.

EXAMPLE

An employee accidentally misplaced a company laptop, which contained a list of 1,000 client records and credit card details.

POLICY RESPONSE

A total cost of $250,000 was paid for the cost of notifying the affected individuals and the Privacy Commissioner of the data breach. This also included the cost of hiring a Public Relations firm to assist the Insured in re-establishing their business reputation.

BizCover for Brokers

Broking Streamlined.

About BizCover for Brokers

BizCover for Brokers is a full lifecycle platform for business insurance that streamlines the end-to-end process for brokers when servicing their SME clients. Created by brokers for brokers, everything we do is about empowering brokers and increasing efficiency.

The B4B platform boasts a broad appetite across 8 products covering over 6,000 occupations. With a single data entry, brokers can compare multiple quotes for multiple products from multiple insurers and bind in minutes. Every broker on the B4B platform also has access to our dedicated Customer Support team for additional assistance when they need it most.

Log in to bind your next policy →

Questions?

Please contact us:

broker@bizcoverforbrokers.com.au

1300 295 262