BizCover for Brokers

Broking Streamlined.

Cyber Threats by Industry

Addressing cyber risks with SME clients in five key sectors

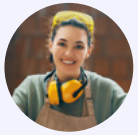
BizCover for Brokers
Broking Streamlined.

Helping SMEs navigate their cyber risk

Small businesses across all industries may be at risk of a cyberattack. But for some, the risk may be larger than they realise.

Let's take a closer look at cyber risk across five key industries:

Allied Health Providers



Manufacturing

Professionals

Tradies

Retailers

ALLIED HEALTH PROVIDERS




Allied Health: A top industry for cybercrime

The "double whammy" of being a small business and working in the healthcare industry could put your Allied Health clients at greater risk than most.

SMEs are a favourite target of hackers—one study found that 43% of cyberattacks are aimed at small businesses[1]. Then there's the healthcare factor. Cyberattacks on this industry rose by 33% during FY22-23[2], making it one of the most attacked in Australia.

Key Threats for Allied Health Providers

- **Ransomware** – Hackers use ransomware to hold vital data hostage until a ransom is paid. This can leave patient records unreachable and bring operations to a standstill.
- **Phishing** – Deceptive emails, texts and phone calls can trick healthcare providers into revealing sensitive information or making payments to fraudulent accounts, a scam that can go undetected for days or weeks.
- **Human error** – Human error, such as emailing sensitive info to the wrong address, could result in fines, penalties or notification obligations for healthcare providers. Human error accounted for 30% of data breaches in Australia in the second half of 2023[3].

ALLIED HEALTH PROVIDERS



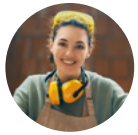

Cyber Liability in Action

Here's a real-life claim example* from one of our insurer partners:

A staff member clicked on a link in a phishing email, which prompted the employee to enter their username and password. Shortly after entering their details, an email blast was sent to all the Insured's staff and people in their address books.

A forensic investigation and review discovered that 115 individuals had their Personally Identifiable Information stolen. They and the OAIC needed to be notified of the breach. The policy paid $110,000 to the Insured.

1. Export Finance Australia, March 2023
2. Cyber Daily AU, 31 July 2024
3. OAIC Notifiable data breaches, July to December 2023

MANUFACTURERS

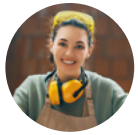


Manufacturing: Making cybersecurity more than an afterthought

A business doesn't need to store sensitive customer data to be the victim of a cyberattack. If a cybercriminal thinks your client will pay a hefty sum to get their systems up and running or restore their supply chain, then they could become a target.

Key Threats for Manufacturers

- **Ransomware** – Hackers can hold a client's operations hostage unless they pay a ransom, causing costly system outages and disruption to their business. Manufacturing was the third-most targeted industry in Australia for ransomware in 2022-23[1].
- **Stolen data** – Cybercriminals may target manufacturers to steal trade secrets or vendor information.
- **Fraudulent payments** – Phishing emails and false billing scams can fool your clients into paying fake invoices or making fraudulent money transfers.

MANUFACTURERS



Cyber Liability in Action

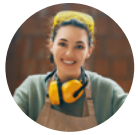
Here's a real-life claim example* from one of our insurer partners:

A manufacturing company's network of 20 computers was affected by ransomware, with users unable to access files that had been encrypted. Threat actors demanded they pay a ransom in exchange for the code to unlock the encrypted data.

The insured's external IT provider was able to recover the lost data from the backup.

Costs were reviewed and accepted by the Insurer, and the Insured was paid under the policy.

1. ASD, Cyber Threat Report 2022-2023

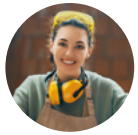

PROFESSIONALS


Professionals: Highly connected and highly at risk

Your SME clients don't have to be an e-commerce business or use the latest cloud technology to become a target. An email address, social media account, or internet-connected device is all a hacker needs to bring a small business to its knees.

Key Threats for Professionals

- **Ransomware** – 28% of reported AU data breaches in 2023 were caused by ransomware[1], a growing threat for SMEs. The professionals, scientific and technical services industry experienced the most ransomware attacks during FY22-23[2].
- **Lost or stolen data** – Human error can also lead to important business or customer info being lost or stolen.
- **Fraudulent payments** – Phishing emails and false billing scams can fool your clients (and their customers) into paying fake invoices or making fraudulent money transfers.

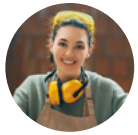

PROFESSIONALS


Cyber Liability in Action

Here's a real-life claim example* from one of our insurer partners:

> *An employee misplaced a company laptop, which contained a list of 1,000 client records and credit card details.*
>
> *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 costs of hiring a public relations firm to assist the Insured in re-establishing their business reputation.*

1. OAIC Notifiable data breaches, January to June 2023 and July to December 2023
2. ASD, Cyber Threat Report 2022-2023

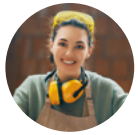
TRADIES

Tradies: More at risk than they might think

Stolen customer data, viruses, and fake payment scams can be devastating for any small business, no matter what industry they are in.

Key Threats for Tradies

- **Ransomware** – Phishing emails and false billing scams can trick your clients into paying phony invoices or making fraudulent money transfers. These are common, with over 108,600 phishing reports made to the ACCC in 2023.[1]
- **Malware** – Viruses and ransomware can lock your clients out of devices, making it impossible to access their network, accept payments, or run their business.
- Data breaches – Sensitive customer data, like credit card details and addresses, can be accessed during a data breach and used to steal money or identities.

TRADIES

Cyber Liability in Action

Here's a real-life claim example* from one of our insurer partners:

> *The Insured received an email from cybercriminals claiming to be one of their suppliers. They asked the Insured to update the supplier's bank details in their system and pay a $70,000 invoice. When the real supplier followed up on the outstanding invoice a week later, the Insured discovered they had been socially engineered.*
>
> *IT forensics confirmed that the Insured's systems were breached, but no data was stolen. The only objective appeared to be social engineering. The Insured's bank was only able to recover $100, and the remaining misdirected funds were indemnified. The Insured's policy paid $85,000 to cover IT assistance and panel forensic work.*

1. ACCC scam statistics 2023

RETAILERS

Retail: Open for business, open to cyberattack?

Retail shop owners do not escape the attention of cybercriminals seeking to snare them in a scam or steal valuable customer data. Cyberattacks can interrupt a small business' operations, whether they're selling online or in a brick-and-mortar shop.

Key Threats for Tradies

- **Phishing** – Fake messages sent by email, SMS or social media are designed to trick your clients into clicking a link, entering login details or transferring money, often by creating a false sense of urgency.
- **Data breaches** – Retailers have both legal and duty-of-care obligations to inform customers of serious data breaches. This process can be expensive and impact your client's brand.
- **Fraudulent payments** – Your clients likely receive a high volume of invoices from vendors and suppliers. Hackers use this to fool retailers into paying fake invoices or sending money to the wrong account. False billing scams resulted in over $27.9 million in losses in 2023.[1]

RETAILERS

Cyber Liability in Action

Here's a real-life claim example* from one of our insurer partners:

> *Cybercriminals impersonated the Insured's bank over the phone and advised they were doing an audit and needed to verify some transactions. The Insured confirmed their login details and security code to authenticate log-in. The cybercriminals used this information to transfer around $80,000 out of the Insured's account.*
>
> *Cover was available for IT forensics to confirm no ongoing unauthorised access was occurring. The bank was able to recover ~ $34,000 of the fraudulent transfers, and cover was available for the remaining ~$46,000.*

1. ACCC scam statistics 2023

BizCover for Brokers
Broking Streamlined.

BizCover for Brokers' Cyber Resources

Refresh knowledge, educate clients, and stay on top of the latest in cyber news.

Cyber Site

Valuable resources and information for you and your brokerage.

Visit now →

Training Suite

5 videos to help you and your staff refresh knowledge of key cyber terminology, risks, and coverage.

Login to watch →

Monthly Digest

Insights, stats, and resources on cyber security and insurance in Australia.

Subscribe →

Cyber Threats Unveiled

A 10-page guide to help you better understand and explain common cyber risks to your SME clients.

Read now →

Editable Question Set

Ask your SME clients to fill out this editable form, so you can process their Cyber quote even faster.

Download →

Our Cyber Insurance Offering

Refresh knowledge, educate clients, and stay on top of the latest in cyber news.

AIG DUAL CHUBB

3 leading insurers

5,000+ occupations covered

$2M

Limits up to $2 million

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 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 Service team for additional assistance when they need it most.

BizCover for Brokers

Broking Streamlined.

Login to bind your next policy →

Questions?

Please contact us:

broker@bizcoverforbrokers.com.au

1300 295 262