BizCover
Insurance made easy

Fact sheet
Cyber Liability Insurance

July 2023

Cyber Liability in a nutshell

If your business is targeted by cyber criminals or suffers a data breach, Cyber Liability insurance will assist in managing incidents from the first notification to response management, forensic investigations, recovery and payment of claims.

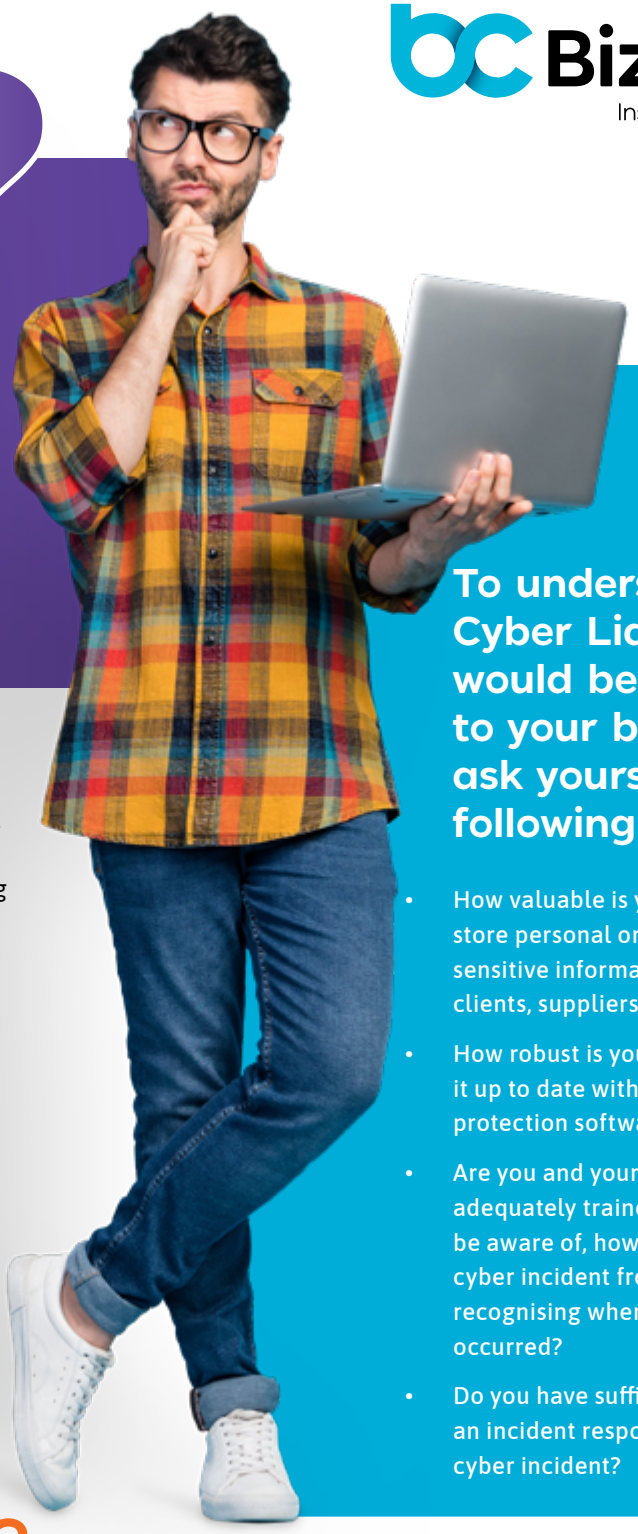
The low-down

Cyber Liability Insurance is designed to help protect you from claims and support your profitability in the event of a cyber breach or attack. Costs associated with defending a cyber claim are also covered.

It offers cover for both third party claims against your business (such as clients suing for breach of privacy, or action taken by the Privacy Commissioner); and first party cover for the expenses your business incurs following a cyber attack (including the costs of repairing and restoring your systems).

BizCover
Insurance made easy

Do you really need it?



Small businesses rely on the internet more than ever. Whether you're storing customer information on a laptop or in the cloud, using an EFTPOS machine to collect payments, sending emails to vendors, or simply updating your website, you could be vulnerable to a cyber attack.

Internet-connected devices and services might be essential to running your business, but they also create an opening for crafty cyber criminals. And not every incident is as sophisticated as a virus or ransomware. Online thieves often use simple phishing emails or fake invoices to fool you or your employees into giving up login details and passwords or making fraudulent payments.

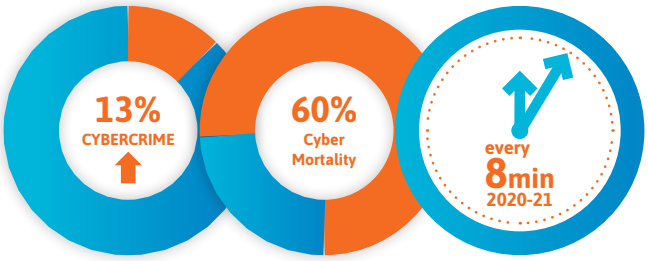
An attack on your business could be a costly experience and has the potential to jeopardise your intellectual property, ruin your reputation and put you out of business.

To understand if a Cyber Liability policy would be beneficial to your business, ask yourself the following questions:

- How valuable is your data? Do you store personal or commercially sensitive information about your clients, suppliers or your own business?
- How robust is your IT infrastructure? Is it up to date with the latest anti-virus protection software?
- Are you and your employees adequately trained on what to be aware of, how to prevent a cyber incident from occurring and recognising when a data breach has occurred?
- Do you have sufficient resources and an incident response plan to manage a cyber incident?

Did you know?

- From 2020 to 21, cybercrime was on the rise, with nearly 13% more cases reported than in the previous financial year. (Australian Government Cyber Security Centre, September 2021)
- Over 60% of Australian SMEs don't survive a cyber-attack or data breach. (The Australian Small Business and Family Enterprise Ombudsman)
- One cyber attack was reported every 8 minutes during the 2020-21 financial year, and they are more substantial than in previous years. (The Australian Cyber Security Centre, September 2021).



Ready to compare?

bizcover.com.au 1300 805 821 hello@bizcover.com.au

BizCover
Insurance made easy

What is typically covered?*

First Party Costs

Covers the costs associated with responding to a cyber incident, including:

- IT forensic costs
- Data recovery costs
- Cyber extortion costs (including ransom demands from hackers)
- Notification and public relations costs

Third Party Losses

Covers your liability to third parties following a data breach, including:

- Claims for compensation
- Legal and defence costs
- Costs arising from investigations by a government regulator
- Fines and penalties for breaching the Privacy Act

Business Interruption

Covers lost profits as a direct result of a cyber event:

- Loss of income
- Business expenses
- Increased cost of operating your business

What is typically not covered?*

- Bodily injury and property damage
- Prior known facts or circumstances Intentional or fraudulent acts
- Damage to computer hardware
- Upgrading of an application, system or network
- Failure or outage of power, utilities, satellites or telecommunication services

Always read the Policy Wording to understand the terms and conditions of Cyber insurance cover, including any applicable exclusions.

Claim Case Study*

An insured hairdresser used a VoIP telephone system for their business. A hacker gained access to the telephone system and made multiple unauthorised calls to a premium number over the course of a month. At the end of the month, the hairdresser received their invoice which included $30,000 of unauthorised calls.

The hairdresser made a claim on their Cyber policy which triggered the optional Social Engineering cover. They were covered for $30,000 of direct financial loss as a result of the phreaking attack.