Surefire
INSURANCE BROKERS | EST 1997

At a glance:

Cyber Insurance

What is cyber insurance?

Cyber insurance is designed to help protect your business from the financial impact of computer hacking or a data breach.

If you see it, report it

In February 2017, the Senate passed the Privacy Amendment (Notifiable Data Breaches) Bill 2016 – setting up a mandatory nationwide data breach notification scheme. This means if you spot a security breach which may cause unauthorised access or disclosure of personal information, you're legally required to report it to the Office of the Australian Commissioner within 30 days. You'll also need to notify the people whose information has been affected.

Who should consider it?

If your business has a website or electronic records, you're vulnerable to cyber hackers. In fact, it's likely that your business will suffer a cyber attack at some stage.

A cyber attack could cost your business more than money. It could also threaten your intellectual property and put customers' personal information at risk – which could damage your reputation.

"Cyber risk primarily refers to the risk posed to a business by a data breach or network compromise. These can occur as a result of either human error, malicious actions by disgruntled employees, by organised crime gangs, acts of war or disruption by nation states."

Insurance Council of Australia, Cyber Insurance: Protecting our way of life, in a digital world, 2022

"Cyberspace has become a battleground."

ACSC annual report July 2021 - June 2022

Did you know?

$97,203

The average loss per cybercrime for medium businesses. This compared to $71, 598 for large organisations and $45,965 for small business.

www.cyber.gov.au (2022-2023)

no.1

Cyber incidents are now considered the top risk facing businesses globally.

Allianz Risk Barometer, 2022

14%

Over the last 2 financial years, the average self-reported cost of cybercrime to businesses increased by 14% each year.

www.cyber.gov.au

What can it cover?

Cyber insurance policies vary in the benefits they provide. Your insurance broker can help you find the most suitable product that meets the needs of your business. Here's the type of cover that your policy may include:

Type of Cover	Potential Benefits
First party losses	
Business interruption losses	Covers financial loss you may suffer as a result of a cyber attack.
Cyber extortion	The costs of a cyber attack, such as hiring negotiation experts, covering extortion demands and prevention of future threats.
Electronic data replacement	The costs of recovering or replacing your records and other business data.
Third party losses	
Security and privacy liability	Damages resulting from data breaches, such as loss of third party data held on your system.
Defence costs	Funds the legal costs of defending claims.
Regulatory breach liability	Covers legal expenses and the costs of fines arising from investigation by a government regulator.
Electronic media liability	The costs of copyright infringement, defamation claims and misuse of certain types of intellectual property online.
Extra expenses	
Crisis management expenses	Provides cover for the costs of managing a crisis caused by cyber hackers.
Notification and monitoring expenses	The costs of notifying customers of a security breach, and monitoring their credit card details to prevent further attacks.

What usually isn't covered?

Exclusions and the excess you need to pay can vary greatly depending on your insurer. Policies generally won't include cover for:

- Damage to computer hardware. Employee entitlements.
- Criminal actions committed by you or your business.
- A cyber attack based on facts of which you were aware.
- Criminals using the internet to steal money from you.

There are other exclusions which your broker can outline for you.

Case Study - Ransomware Attack

An employee opened an email that they believed to have been sent from Australia Post about a package delivery. Within 10 minutes every computer in the business was locked and a blue screen appeared with a demand to pay $120,000 to the hacker to unencrypt the data.

As the business held client information, (names, addresses etc) they needed to notify them of the breach of data by mail at a cost of $50,000. It took two weeks to arrange payment with the hacker and restore data. This interruption to the business cost a profit loss of $45,000.

The nearest competitor found out about the cyber-attack and notified local news outlets and the company's reputation began to suffer. A Public Relations expert was engaged to improve their public image at the cost of $45,000.

A comprehensive Cyber policy would cover the whole loss of $260,000.

Surefire
INSURANCE BROKERS | EST 1997

PERTH
Level 1/297 Vincent Street
Leederville WA 6007
info@surefireib.com.au
08 9224 9555

KALGOORLIE
104 Hannan Street
Kalgoorlie WA 6430
info@surefireib.com.au
08 9021 6524

Surefire Insurance Brokers Pty Ltd | ABN 33 664 956 567 | AFSL 554324

surefireib.com.au