Cyber protection insurance at a glance

What is cyber protection insurance?

Cyber protection 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

Did you know?

$33,442

The average loss per cybercrime for medium businesses. This compared to $19,306 for large organisations and $8,899 for small businesses.

(Australian Cyber Security Centre, Annual Cyber Threat Report, 2020-21)

#1

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

(Allianz Risk Barometer, 2022)

13%

Cyber crime reports increased nearly 13% between the 2019-20 and 2020-21 financial years.

(Australian Cyber Security Centre, Annual Cyber Threat Report, 2020-21)

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.
- 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 insurance broker can outline.

Case Study

Your employee opens an email attachment infected with a ransomware virus. Access to your systems and data are blocked and the virus software informs you that it will remain unavailable unless you pay the ransom amount. Rather than paying the hacker and opening your business up to further extortion attempts, you hire external IT consultants to recover your back-up data and files and upgrade your antivirus software.

Over the week it takes to apply these fixes, you have to close your business, causing you to lose revenue. It also affects your reputation with your clients; one of your clients threatens to sue you for the delay which cost them a large amount of money.

A Cyber Protection Insurance policy allows you to recover some of the costs you incur during this incident. Depending on your policy, you may be able to make a claim for losses caused by the interruption to your business, the costs of recovering your data and upgrading your software, and ongoing crisis management expenses.

Contact us today

Knightsbridge Insurance Group

Kirsty Macleod

1300 527 4343

kirsty@knightsbridgeinsurance.com.au

www.knightsbridgeinsurance.com.au

ABN: 41 627 300 341 | **AFSL:** 514855

Knightsbridge Insurance Group Pty Ltd

Steadfast