
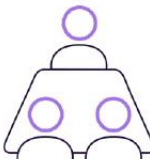
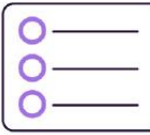


How Cyber Insurance protects your business

Cyber Insurance is pivotal in helping a business recover after a cyber attack. With organisations increasingly reliant on technology, digital products and third-party services, there are a number of ways your business can be compromised in a cyber attack.

Outlined below are some key methods of attack, accompanied by insurance claim scenarios to demonstrate how Cyber Insurance can respond to protect your business.

TYPE OF CYBER ATTACK	CYBER INSURANCE CLAIM SCENARIO	CYBER INSURANCE RESPONSE
 <p>Hacking A crime involving an attempt to exploit a computer system or private network by gaining unauthorised access to, or control over network security systems for an illicit purpose.</p>	<p>A retail clothing store operated an E-commerce website which became infected with malicious code. As a result the website showed black screens to customers and staff were unable to access orders in the system.</p>	<p>Provides cover for:</p> <ul style="list-style-type: none">• Removal of the malware and restoration of the website• Lost revenue and increased costs caused by the attack
 <p>Cyber Extortion Crime involving an attack or threat of attack against your IT infrastructure, coupled with demand for money to stop the attack.</p>	<p>A malicious actor pretending to be tech support gained access to a manufacturing plant's computer systems. This enabled them to pose as an insider, eventually gaining access to highly restricted information including customer data, bank details and other sensitive personal information. The hacker threatened to sell trade secrets to competitors and banking details on the black market, and make sensitive personal information public - unless the insured company paid.</p>	<p>Provides cover for:</p> <ul style="list-style-type: none">• IT forensics, crisis management and public relations• Notification costs, credit and identity monitoring• Pursuit costs against the perpetrator• Mandatory data breach notifications, including notice to regulators because of the manufacturer's failure to keep information secure• Defence and settlement costs for third party claims made against the insured
 <p>Privacy Error People make mistakes! Unintentional employee actions can directly compromise a company's IT systems and data security.</p>	<p>An employee of a medical practice sent an administrative email to patients advising of altered trading hours over the Christmas period. However, the employee inadvertently attached an excel spreadsheet to the email that provided personal information of some patients. The spreadsheet included patients name, address, Medicare number and a short description of their last visit.</p>	<p>Provides cover for:</p> <ul style="list-style-type: none">• Notification costs which includes the cost of notifying the individuals impacted and notifying the Office of the Australian Information Commissioner or other authorities (such as medical authorities).• Identity theft response costs to the third parties impacted by the privacy error

TYPE OF CYBER ATTACK	CYBER INSURANCE CLAIM SCENARIO	CYBER INSURANCE RESPONSE	
	<p>Social engineering</p> <p>The term used for a broad range of criminal activities accomplished through human interactions. Using psychological manipulation, perpetrators trick victims into making security mistakes or divulging sensitive information.</p>	<p>A medical centre received communications from a fraudster impersonating the ATO requiring urgent payment of outstanding taxes. The medical centre paid the 'outstanding' taxes in good faith having believed the demand was genuine.</p>	<p>If Criminal Financial Loss coverage including Socially Engineered Theft is applicable, the lost funds are covered, including investigation costs. This cover is often an optional extra.</p>
	<p>Malware attack on a supplier</p> <p>A method of attack where cybercriminals create malicious software that's installed on someone else's device without their knowledge, to gain access to personal information or to damage the device, usually for financial gain. Different types of malware include viruses, spyware, ransomware, and Trojan horses.</p> <p>If one of your key suppliers falls victim, it can impact your business operations, cost of doing business and profits.</p>	<p>An external supplier of a bedding manufacturer suffers a malware attack. Their 'Just In Time' manufacturing plant grinds to a halt for three weeks while engineers and IT experts scrambled to restore systems and production. As a result of the supplier's cyber event, the insured could not source critical components and manufacturing operations were interrupted.</p>	<p>If Contingent Business Interruption cover is applicable, insurance would pay for the impact on the bedding manufacturer's business costs arising from the external suppliers' outage. This cover is often an optional extra.</p>

About Cyber Insurance

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

This risk exposure is not covered by a traditional business insurance policy.

Who needs Cyber Insurance?

Any business with a website or electronic records, or an IT system that connects to the internet is vulnerable. IT security systems are simply not enough in the digital era.

Like any vaccination, current anti-virus software protects you from what is known, not what is not. That means SMEs need stronger protective measures to defend against ever-changing and ever-present cyber attacks ([Emergence](#)).

What's covered?

FIRST PARTY LOSSES

- Business interruption losses, for the business and external suppliers
- Cyber-extortion
- Electronic data replacement

THIRD PARTY LOSSES

- Security and privacy liability
- Legal defence costs
- Regulatory breach liability
- Electronic media liability

ADDITIONAL EXPENSES

- Crisis management expenses
- Notification and monitoring expenses

We're here to answer your questions whenever you need us.



Westphalian Insurance Brokers

N Karlene Lykiard
p 0459 990 058
e Karlene@westphalian.com.au
w www.westphalian.com.au



**AUTHORISED
BROKER**

Community Broker
Network Pty Ltd

ABN 60 096 916 184 | AFSL 233750