Why you need cyber insurance

If you have an internet connection, you're at risk from a cyber attack which could have a disastrous impact on your business.

What is cyber insurance and cyber risk?

Not a day goes by without a cyber attack or data breach hitting the headlines. Businesses in all industries, and of all sizes, are being targeted more than ever by online threats.

You may think that these attacks will never happen to you but, unfortunately, that isn't the case. According to Norton, more than 500, 000 small businesses fell victim to a cyber attack in 2017 – and that number keeps rising.

Cyber security is the best first step to ensuring you stay protected online, but cyber insurance plays an important role in helping you get back on your feet.

Cyber insurance acts in the same way as any other insurance policy – it helps you pick up the pieces in the aftermath of an event. A cyber insurance policy can cover your business from a variety of threats and gives you access to a host of experts to help you contain, control and recover from an attack.

A cyber hack happens every **39** seconds [1]

More than **one third** of attacks are due to **human error** [2]

200,000 computers, **150** countries

the estimated size of **Wannacry**, one of the **biggest cyber attacks** in history which hit in 2017 [3]

Fail to plan, plan to fail

Know your risk

If you don't know what's at stake in your business, how can you protect it? Start by understanding what the most important aspects of your business are and the risk they face. Our cyber specialists can help guide you to protect your risk.

Manage your risk

Working with cyber security providers and cyber risk specialists can help you decide on the best way to protect your business. Staff training is also a really important aspect of preparation as they are often the weakest link in a system.

Transfer your risk

Sometimes things can go wrong no matter how well prepared you are and this is where insurance plays such a vital role. It could be the difference between you re-opening your doors or shutting for good.

1. safeatlast.co/blog/cybercrime-statistics/
2. Notifiable Data Breaches Scheme 12-month Insight Report
3. https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX
4. Cyber Security Review, Department of the Prime Minister and the Cabinet.
5. 2019 Verizon Data Breach Investigations Report /http://mastersinlaw.champlain.edu/internet-privacy-in-the-digital-age/
6. 2018 Cost of a Data Breach Study by Ponemon

Most common cyber attacks

Phishing and Social engineering

This is where an attacker pretends to be someone known to your organisation in a bid to gain access to your files or be paid by your staff unknowingly.

Malware

Means malicious software. Any program or file that is harmful to a computer user. Things such as viruses are malware and can allow cyber attackers to access or shut-down your network.

Ransomware

A type of malware that is designed to shut you out of your computer or network until you pay a ransom to an attacker. Famous attacks such as WannaCry used ransomware on a huge scale.

Human error

Human error is one of the most common reasons that a cyber attack or data breach takes place. Train your staff so they know what to do, and what not to do, online.

Cybercrime costs the Australian economy up to **$1 billion** each year [4]

61% of breaches hit SMEs and **60%** of those impacted are **out of business** within **six months** of an attack [5]

In 2018, Australia saw the average cost of a **data breach rise** by over **5%** [6]

How could cyber insurance help my business?

Prepare
Our cyber specialists help you identify the biggest risks you face, and the things you most need to protect.

Threats
Cyber insurance covers you from a range of threats including human error, ransomware, malware and social engineering.

Expertise
Cyber insurance gives you access to a suite of experts, from legal or PR advice to IT specialists and IT forensics.

Response
If your business is forced to close after an attack, cyber insurance helps you pay the bills during any outage.

What to do next

Want to find out more about your cyber risk and how cyber insurance could help you? **Our cyber specialists are here to help.**

Alberto Piccenna
Client Manager, Professional & Financial Risks
P: 02 9242 2076
M: 0466 928 955
E: alberto.piccenna@ajg.com.au

Robyn Adcock
Cyber/Technology Practice Leader
P: 02 9242 2008
M: 0414 971 918
E: robyn.adcock@ajg.com.au

Gallagher

Insurance | Risk Management | Consulting

ajg.com.au/cyber

Arthur J. Gallagher & Co (Aus) Limited. Operates under AFSL No. 238312. To the extent that any material in this document may be considered advice, it does not take into account your objectives, needs or financial situation. You should consider whether the advice is appropriate for you and review any relevant Product Disclosure Statement and policy wording before taking out an insurance policy. Our FSG is available on our website, www.ajg.com.au. Arthur J. Gallagher & Co (Aus) Limited. ABN 34 005 543 920, Level 12, 80 Pacific Highway, North Sydney, NSW 2060. REF2563-0819-V1.5