



Cyber Insurance



WHY CHOOSE MEDIPROTECT?

We provide insurance broking and risk advisory services to thousands of small to medium organisations, associations and individuals across Australia. Our goal is to provide a valued service to our clients that, through tailored advice and exceptional service, delivers an insurance program that protects when a claim arises.

With offices across Australia, we understand the local challenges which allow us to proactively address the unique requirements of your insurance. We use our considerable buying power to negotiate with underwriters and our collective experience to ensure you're appropriately covered to your needs and budget. We understand the commercial realities that affect your business and tailor your insurance program to best suit those requirements.

We care. You're Protected.

Mediprotect is a division of publicly listed PSC Insurance Group Limited (ASX: PSI). As part of PSC Insurance Group focuses on being the trusted insurance and risk management partner for its diverse range of Small to Medium Enterprise (SME) clients. A publicly listed insurance intermediary business, PSC Insurance Group has a proven track record protecting the business and personal assets of our clients.

The cyber threat facing Australia is undeniable and unrelenting, an issue that once only concerned IT security professionals now extends to the boardroom, to shareholders and to individuals. The need for strong cyber security measures has never been greater, with the rise of sophisticated and targeted malicious activity against Australia's networks.

Cyber insurance is designed to help protect your business from the financial impact of computer related breach or intrusion event.

WHY DO I NEED IT?

If your business has a website or electronic records, you're vulnerable to a cyber event. The risk of suffering cyber events have increased significantly in recent times. A cyber event could cost your business more than just money. It could also threaten your reputation, intellectual property and put customers personal information at risk.

IF YOU SEE IT, REPORT IT?

In February 2018, the Notifiable Data Breaches Scheme became active. This means that if you suffer a data breach that results in unauthorised access or disclosure of personal information, you may be required to report it to the OAIC within 30 days.

You may also be required to notify the people whose information has been affected.

CASE STUDY

Your employee opens an email attachment infected with ransomware. Access to your systems and data are locked and the virus software demands payment of a ransom to unlock.

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 upgrade your anti-virus software.

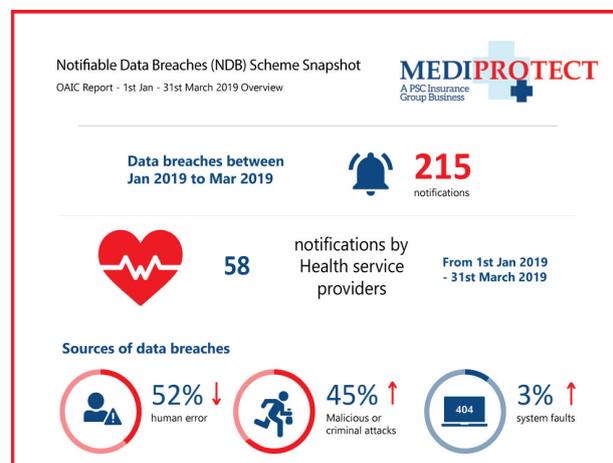
In the week it takes to implement this strategy, you lose revenue. It also affects your reputation with your clients with one of them threatening to take legal action.

Having a Cyber policy in place would mean you make one notification to a 24/7 emergency line that would give you immediate access to specialised IT security and legal assistance. Depending on your policy, you may also then be able to make a claim for losses incurred as a result of the interruption to your business.

MediProtect has been providing innovative financial service solutions to healthcare professionals, medical and affinity groups since 1999. Data Breach and Cyber Crime policies are designed for healthcare practices and can cover you for:

Response Management	Costs associated with Legal, IT, PR, Data Restoration, Notification & Credit/Identity Theft Monitoring
Data Protection	Costs associated with Data Protection & Regulatory Investigations
Data Liability	Third party liability and compensation claims arising from an insured data breach
Business Interruption	Coverage can be tailored to also include business interruption as a result of an insured breach
Cyber Extortion	Cover can be extended to cover losses relating to Cyber Extortion
Outsourced Service Providers	Coverage can be arranged to respond to security failures of outsourced service providers

Policy response will generally include investigative and legal defence costs. Cover may also extend to certain fines and penalties arising from any regulatory investigations. Contact your insurance advisor to discuss coverage.



WHAT NEXT?

for more information or advice.



Call us on 1800 177 163.



Email us at admin@imga.com.au



Visit www.mediprotect.com.au
Where you can request a quote or read more about us.

Follow us 