


Cyber liability insurance safeguards businesses against financial losses stemming from cyberattacks or data breaches. In Australia, as elsewhere, the risk of cyber threats is substantial, and businesses of all sizes can be vulnerable. Despite costing Australian businesses \$1 billion annually, cybercrime remains one of the least insured areas.

# CYBER LIABILITY INSURANCE EXPLAINED

The healthcare sector is particularly vulnerable to cyberattacks due to the sensitive nature of the data it collects and stores. While all businesses face cyber risks, historical data indicates that the healthcare sector is twice as likely to be targeted compared to other industries. By obtaining cyber liability insurance, practices can mitigate the financial risks associated with cyberattacks and protect their operations and reputation.

## Key Coverage of Cyber Liability Insurance:

<b>Data Breach Response Costs:</b>	Covers the expenses incurred in responding to a data breach, including legal fees, forensic investigations, public relations, and notification costs.
<b>Third-Party Liability:</b>	Protects the business from lawsuits brought by individuals or other entities affected by a data breach.
<b>Business Interruption</b>	Covers the loss of income or profits resulting from a cyberattack that disrupts business operations.
<b>Cyber Extortion:</b>	Provides coverage for ransom payments or other expenses related to cyber extortion threats.
<b>Media Liability:</b>	Protects the business from claims related to defamation or copyright infringement.

 **HINT** Cyber insurance, is often offered as an add-on to other policies like Management Liability and Professional Indemnity, and typically don't provide adequate coverage. These 'tack-on' policies typically have limited coverage limits and restrictive terms, making them less suitable for healthcare businesses who face significant cyber risks. In the majority of circumstances, a stand-alone policy is required to ensure appropriate levels of cover and protection.

## CYBER LIABILITY INSURANCE WHY IS IT ESSENTIAL

Emerging trends highlight the importance of cyber liability insurance for businesses. Below are some key areas a quality policy can address.

### Rising Threat Landscape:

Cybercriminals are increasingly targeting businesses worldwide, including in Australia. Their attacks are becoming more sophisticated and harder to defend against. Healthcare practices and clinics are prime targets. With a cyberattack occurring every eight minutes, it's a matter of when, not if, your business will be impacted.

### Data Privacy Laws:

Australia's stringent data privacy laws, such as the Privacy Act 1988, are designed to protect individuals' personal information. These laws regulate how businesses collect, use, store, and disclose personal data. Non-compliance with these laws can result in significant penalties, including fines, public reprimands, and legal action.

### Reputational Damage:

A data breach can severely damage a business's reputation, leading to customer loss and financial losses. A quality Cyber Liability policy can mitigate and address this risk.

### Regulatory Fines:

Non-compliance with data privacy laws can result in substantial fines and penalties for both Practice Owners and the company. Additionally, regulatory authorities may impose directives requiring public notification and costly financial monitoring for affected individuals.

### Business Interruption:

Being locked out of your software systems and unable to access critical information and data can disrupt your business operations and lead to significant financial losses.

### Human Error

Human error remains the primary cause of cyber and data breaches, accounting for more than half of all incidents. While external threats are crucial to address, business must also prioritize employee training and internal access controls to mitigate the risks posed by human factors.

## Best Practice Controls



Insurers expect, and require businesses to have the minimum best practice standards in place. To complement your Cyber Liability insurance, a comprehensive risk mitigation plan is essential. Consider implementing these practical measures to protect your practice:

- Regularly, and frequently back up all systems. It is important to test and check backups for data integrity to ensure that are working properly and can be used if necessary
- Provide annual cybersecurity training for both medical and non-medical staff, annual training should address any emerging threats
- Enable strong spam filters and 2FA (two-factor authentication) protocols.
- Invest in technologies that can scan emails for suspicious activity and isolate them for review in a safe environment.
- Limit access to sensitive folders and information on your systems, only allowing access those who need it.
- Conduct regular penetration tests.
- Improve password management and ensure passwords are changed at least every 45 days.