Cyber Insurance

What is it?

Technology has never been so deeply entwined in our businesses. While it delivers significant efficiencies and convenience, it also comes with significant cyber risks. Many business owners don't fully understand how their business could be attacked. While others think they don't have a cyber exposure at all, due to their industry or size. The reality is anybody who collects data or uses a computer with the internet is at risk. Something as simple as an employee clicking on the wrong link, sending an email to the wrong person or using a corrupted website could leave your entire system exposed. Cyber Insurance is one of your best forms of defence.

Government estimates suggest cybercrime costs the Australian economy more than $1 billion every year with nearly half of these attacks focused on SMEs, simply because of their vulnerability. Of those that are attacked, approximately 60% will close their doors within six months as a direct result of the data breach.

Notifiable Data Breaches Scheme

The Notifiable Data Breaches Scheme came into effect in early 2018 and places added compliance pressures on business owners. It is now mandatory for any qualifying business to notify a cyber breach to all affected parties, as well as the Australian Privacy Commissioner. This legislation is applicable to Australian Government agencies, businesses and not-for-profit organisations with an annual turnover of $3 million or more, credit reporting bodies, health service providers and TFN recipients, among others.

What it covers?

There are many types of Cyber Insurance now available. Some of the key inclusions to look for are listed below.

First Party Loss

- Incident response costs
- Business income loss
- Data restoration
- Breach response costs
- Notification costs
- Legal defence costs
- Cyber extortion
- Regulatory fines and penalties
- Payment Card Industry (PCI) fines, penalties and assessments
- Cyber reputational harm

Third Party Loss

- Security and Privacy Liability

What can you do right now?

To fully protect yourself and your business, the first steps are to focus on risk management and awareness within your organisation. Simple things such as developing a strong password policy, conducting regular training about cybersecurity, updating IT equipment and security software and creating an incident response plan are essential. The other critical step is to take out an appropriate level of cyber risk insurance.