SherpaTech
INSURANCE SPECIALISTS FOR TECH & IT

DOES YOUR COMPANY NEED CYBER INSURANCE?

Our self-assessment Cyber Insurance Check List has been created to assist MSPs in assessing whether or not cyber insurance is needed. Please note that the decision to secure cyber insurance may be impacted by additional requirements, including the industry that you support, requirements under contract, regulatory regimes, jurisdiction and more.

There are three stages to the Cyber Insurance Check List:

1. Getting house in Order **2. Do I have these things?** **3. What should I look for in Cyber Insurance?**

1. GETTING HOUSE IN ORDER	INFORMATION OR LINK	COMPLETED
• Patch and update management	Software patches, updates and policies are up to date	Y N N/A
• User Training	Regular cyber security training for staff and stakeholders who access your systems	Y N N/A
• Multi Factor Authentication - MFA	MFA in place across all platforms. View our MFA Checklist here	Y N N/A
• Endpoint Protection	Endpoint protection including firewalls, anti-malware and more are in place and up to date	Y N N/A
• Authorisation of Payments	Processes for transactions and approvals for any changes to payment details	Y N N/A
• Data Backups	Data backups are in place and regularly tested	Y N N/A
• Data breach Procedure – Documented and understood	View our Data Breach checklist here	Y N N/A

The above is typically a minimum insurance requirement. Any security posture over and above is often looked at favourably by insurers (such as ISO, Essential 8 etc.). sharing this information with insurers will enhance risk attractiveness.

2. DO YOU HAVE THESE THINGS	WHY	COMPLETED
• Do you carry PII (personal identifiable information)	OAIC	Y N N/A
• Do you manage client data?	You may be responsible	Y N N/A
• Do you manage business-sensitive data?	You may be responsible	Y N N/A
• Is your annual turnover more than $3M AUD?	OAIC	Y N N/A

If you answered "Yes" to any of the above, you should consider Cyber Insurance.

Consider engaging a reputable insurance broker to assist with this section.

3. WHAT SHOULD I LOOK FOR IN EVALUATING CYBER INSURANCE?	NOTES	RATING
A. How the policy responds to cyber incidents		1 2 3
a. Regarding remediation		1 2 3
b. Business interruption		1 2 3
c. Fines and penalties		1 2 3
d. Brand damage		1 2 3
B. Impact of insurance excesses		1 2 3
C. Impact of waiting periods		1 2 3
D. Impact of cyber exclusions		1 2 3
E. Impact of cyber endorsements		1 2 3
F. Impact of crime and social engineering coverage		1 2 3
G. Importance of cover levels meeting customer or other contractual requirements		1 2 3
H. Does the policy include contractors?	View our Contractor checklist here	1 2 3

1 - Low
2 - Medium
3 - High

If any of the above areas are rated High, it is important to have these explained by an insurance professional.

At SherpaTech we are specialists in Tech and IT Insurance Risk and we are here to help.

A GOOD CYBER INSURANCE POLICY SHOULD INCLUDE AS A MINIMUM

- Incident Response 24/7
- Legal Representation
- Communication Specialist
- Negotiation specialist
- Forensic Specialist

FIRST PARTY LOSSES

- Cyber event response costs
- Losses to your business
- Business interruption

THIRD PARTY LOSSES

- Defense costs
- Fines and penalties

CRIMINAL FINANCIAL LOSS

- Cyber theft
- Social engineering theft

www.sherpatech.com.au | 1800 803 201 | Australia-wide Service