



# Cyber Insurance Pitfall Prevention Checklist

Your Actionable Guide to Ensuring  
**Full IT Protection** for Your Business

Downloading this document to your device is highly recommended

# Table of Contents

## I. Introduction

- The Truth About Cyber Insurance: Are You Really Covered?
- How This Guide Helps

## II. Checklist: Evaluate If Your Insurance is Really Protecting You

- Getting House in Order
- Do You Have These Things?
- What Should You Look for in Evaluating If Your Business Needs to be Cyber Insured

## III. Taking Action

- How to secure your business with confidence

I.

# Introduction

# The Truth About Cyber Insurance: Are You Really Covered?

In today's digital landscape, small and medium-sized businesses (SMBs) in Australia face increasing cyber threats. While cyber insurance offers a safety net, it's crucial to understand that not all policies provide the protection you might expect. Hidden exclusions, specific security requirements, and complex policy terms can leave your business vulnerable when you need coverage the most.

This guide aims to help you assess your business and help you identify if you are in need of a cyber insurance, and if so, what should you look for to avoid the common pitfalls of cyber insurance, ensuring your policy aligns with your cybersecurity needs. By following this checklist, you'll gain a clear understanding of what to look for, what to avoid, and how to ensure comprehensive coverage in the event of a cyber incident.

## How This Guide Helps

**This checklist covers three key areas:**

1. **Getting house in order** – Fundamental security measures that insurers expect, such as patch management, MFA, endpoint protection, and data breach response plans.
2. **"Do You Have These Things?"** – Factors that may influence the need for cyber insurance, including handling sensitive data and meeting industry compliance requirements.
3. **Evaluating a Cyber Insurance** – Key aspects to consider when selecting a policy, including coverage for business interruption, legal expenses, and financial losses from cyber incidents.

The self-assessment cyber insurance Checklist, with the help of SherpaTech, has been created to assist you in assessing whether or not your business' cyber insurance has the right coverage, or help you identify if you really need one.

**II.**

# **Checklist: Evaluate If Your Insurance is Really Protecting You**

## Steps to Cyber Insurance Confidence

### Step 1: Getting house in order



#### 1. Patch and update management

Making sure that software patches, updates and policies are up to date



#### 2. User Training

Regular cyber security training for staff and stakeholders who access your systems



#### 3. Multi Factor Authentication - MFA

MFA in place across all platforms. Use Sherpatech's MFA checklist by [clicking here](#)



#### 4. Endpoint Protection

Endpoint protection including firewalls, anti-malware and more are in place and up to date



#### 5. Authorisation of Payments

Processes for transactions and approvals for any changes to payment details



#### 6. Data Backups

Data backups are in place and regularly tested



#### 7. Data breach Procedure – Documented and understood

Use Sherpatech's Data breach Checklist by [clicking here](#)

### Need Help? Have Questions?

Don't hesitate to reach out. Click the button below.

[Contact Us Now](#)

Steps to Cyber Insurance Confidence

Step 2: Do You Have These Things?

- ☐ Do you carry PII (personal identifiable information)  
Why? Because of: OAIC
- ☐ Do you manage client data?  
Why? Because you may be responsible
- ☐ Do you manage business-sensitive data?  
Why? Because you may be responsible
- ☐ Is your annual turnover more than \$3M AUD?  
Why? Because of: OAIC

Step 3: Evaluating a Cyber Insurance

low	mid	high	
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	How the policy responds to cyber incidents
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Impact of insurance excesses
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Impact of waiting periods
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Impact of cyber exclusions
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Impact of cyber endorsements
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Impact of crime and social engineering coverage
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Importance of cover levels meeting contractual requirements
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Impact of crime and social engineering coverage

\*If any of the above areas are rated High, it is important to consult a professional.

Need Help? Have Questions?

Don't hesitate to reach out. Click the button below.

Contact Us Now

III.

# Taking Action



### III. Taking Action

## Secure Your Business' Future with Confidence

Cyber threats are unpredictable, and the financial impact of an attack can be devastating. Ensuring your business has the right security measures in place – and that your cyber insurance policy provides adequate protection – is essential to mitigating risk. By following this checklist, you can identify gaps in your cybersecurity posture, assess your insurance needs, and take proactive steps to safeguard your business.

At FusionRed, we help businesses strengthen their cyber resilience and navigate the complexities of cyber insurance. Our team can thoroughly assess your security framework, recommend improvements and what your next actions should be, and ensure your policy aligns with your business risks.



### Exclusive FREE CONSULTATION

Schedule a free consultation today and take the first step toward securing your business.

**Click the button below to schedule a call**

**Contact Us Now**

