

Cyber Risk Self-Assessment for Australian SMEs

Tick each box that applies to your business. The more boxes left unticked, the more exposed you could be.

YOUR TECHNOLOGY & DATA USE

- ☐ We use email to communicate with clients and suppliers
- ☐ We store customer or staff data (e.g. names, contact info, bank details)
- ☐ We use cloud-based software or SaaS platforms
- ☐ We accept card payments or online transactions
- ☐ We rely on our IT systems to operate daily
- ☐ We limit who has access to sensitive data based on role
- ☐ Our Wi-Fi networks are encrypted and password protected
- ☐ We automatically install security updates and software patches

YOUR PEOPLE & PRACTICES

- ☐ Our staff are trained in cyber safety (e.g. phishing awareness)
- ☐ We conduct refresher training at least once a year
- ☐ We use strong passwords and multi-factor authentication (MFA)
- ☐ We have internal data security policies
- ☐ Devices are protected with antivirus/endpoint protection
- ☐ We regularly back up our data offsite or to the cloud

- ☐ Personal and business devices are kept separate
- ☐ We review and revoke access for former staff or contractors promptly

YOUR INCIDENT READINESS

- ☐ We have an incident response plan
- ☐ We run simulations or tabletop exercises for breach scenarios
- ☐ We have a contact list for IT, legal and cyber insurance support
- ☐ We know who to call if there's a breach or ransomware attack
- ☐ We have Cyber Insurance in place
- ☐ We know what our cyber policy covers and excludes
- ☐ We have confirmed our business interruption coverage includes cyber-related outages
- ☐ We know our legal obligations if a breach occurs
- ☐ We've reviewed our risks with a broker in the last 12 months

This checklist is provided as general information only and is intended to help Australian small to medium businesses self-assess common areas of cyber risk. It does not take into account your specific business operations, systems, or risk profile.

Completing this checklist does not guarantee coverage under a cyber insurance policy or compliance with any legislation or regulatory requirements.

We recommend speaking with your insurance broker or a qualified cybersecurity professional to assess your individual circumstances and determine appropriate insurance solutions.

Recovering from a cyber incident without the right insurance can be costly, both financially and reputationally.

Let us help you find a policy that suits your business needs.

steelpacific.com.au

ABN: 47 075 780 353

AFSL: 230634



This is general information only and does not consider your individual objectives, financial situation or needs. Always consult a broker before making a decision. Policies are subject to terms, conditions, and exclusions. For more information and to explore insurance solutions, contact your local broker.

©Ballyglisheen Pty Ltd trading as Steel Pacific Insurance Brokers