Cyber Maturity Assessment Questionnaire

A comprehensive checklist for evaluating your organisation's cyber security posture. This assessment covers critical business, technical, and compliance requirements that cyber insurers need to understand your risk profile.

IMPERIUM
CYBER SECURITY

Business Foundation & Compliance

Understanding your business structure and regulatory compliance is essential for assessing cyber risk exposure and insurance requirements.

1

Business Profile

- Number of endpoints/users/employees (PCs/laptops only)
- Business size: Small (5-20), Medium (20-80), or Large (80-200)
- Number of office sites and geographic locations
- Number of private/local networks (enter 0 if entirely cloud-based)
- Annual turnover/revenue

2

Core Policies & Plans

- Information Security Policy in place? ☐ Yes ☐ No
- Business Continuity Plan (BCP) or Disaster Recovery Plan (DRP)? ☐ Yes ☐ No (Date last tested: _____)
- Incident Response Plan (IRP) in place? ☐ Yes ☐ No
- Notifiable Data Breach Plan in place? ☐ Yes ☐ No

3

Regulatory Compliance

- Australian Privacy Act & Privacy Principles (PII - Personal Identifiable Information)? ☐ Yes ☐ No
- Notifiable Data Breaches (NDB) & OAIC compliance? ☐ Yes ☐ No
- Payment Card Industry Data Security Standard (PCI DSS)? ☐ Yes ☐ No
- General Data Protection Regulation (GDPR)? ☐ Yes ☐ No
- Sarbanes-Oxley Act (SOX)? ☐ Yes ☐ No
- Children's Online Privacy Protection Act (COPPA)? ☐ Yes ☐ No

4

Incident History

Have you suffered a cyber attack before (virus, ransomware, DoS/DDoS, malicious internal actor, phishing, etc.)? ☐ Yes ☐ No

If yes, provide details: What type? _____ Where? _____ When? _____

Endpoint Protection & Access Control

These fundamental security measures protect individual devices and user access points—the primary targets for cyber attacks.

Device Security

- ☐ Antivirus installed on each user endpoint
- ☐ Password Manager for each endpoint user
- ☐ Multi-Factor Authentication (MFA) for each endpoint user
- ☐ VPN (Virtual Private Network) installed on each user endpoint

Backup & Recovery

- ☐ Automated image backup of all endpoints on-premise (Frequency: ☐ Daily ☐ Weekly, Date last tested: _____)
- ☐ Automated file backup of all endpoints to cloud (Frequency: ☐ Daily ☐ Weekly, Date last tested: _____)
- ☐ Backups are segmented (isolated from main network)

Microsoft 365 Security

- ☐ O365 is used across the business
- ☐ O365 MFA is enabled
- ☐ O365 Privileged Access Management (PAM) is enabled

Remote Access

- ☐ Remote Desktop Protocol (RDP) is in use/able to be used

IMPERIUM
CYBER SECURITY

Network Security & Monitoring

Advanced security measures that detect, prevent, and respond to threats across your network infrastructure.

Threat Detection & Monitoring

- ▯ Real-time intrusion detection
- ▯ Network security monitoring
- ▯ System logging
- ▯ Traffic geo-tracking
- ▯ Security and Information Event Management (SIEM)
- ▯ Threat identification
- ▯ File integrity monitoring
- ▯ Incident notification and alerting

Vulnerability Management

- ▯ Vulnerability identification (scheduled scans, reporting, on-demand dashboard)
- ▯ Patch detection for operating systems
- ▯ Patch detection for applications

Data Protection

- ▯ Data encrypted at rest (particularly backups)
- ▯ Data encrypted in transit
- ▯ Data Loss Prevention (DLP) technology

Network Perimeter Security

- ▯ Firewalls in place to secure network
- ▯ Suitable firewall rules in place to optimise firewalls
- ▯ Inbound email authentication (DMARC, DKIM, SPF, etc.)

Next Steps: Complete this questionnaire thoroughly, marking each checkbox and providing requested details. Unknown answers should be clearly marked as "Unknown" for follow-up investigation. This assessment forms the foundation of your cyber insurance application and security improvement roadmap.