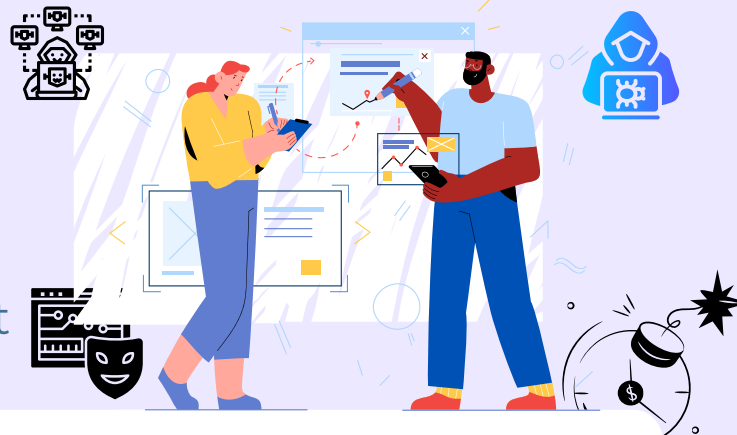# Cyber Resilience

Breach **Minimisation** Checklist

1 What is your RISK EXPOSURE?

☐ How much private, sensitive, and regulated data resides on endpoints over past 8+ years and what is its value in dollars?

☐ Who are the top 3 people with the greatest risk exposure and what is their data risk value?

☐ Would you like your stale data made useless to a hacker - even if it stolen?

2 How EASY are you to breach?

☐ Up to 60% of breaches leverage known vulnerabilities - How many critical vulnerabilities do you have **right now** - **TODAY**?

☐ With over 3,300 new vulnerabilities every month that a hacker or **bot** can and **will** use to breach you - How often do you scan for new vulnerabilities? Note: It should be continuously.

☐ Would you like continuous vulnerability scans **with** remediation to reduce your risk of a breach and having data stolen by closing your doors and windows to bots and hackers?

3 Are you aware of the proposed updates to Privacy Laws?

☐ $66,000 (individual) or $330,000 company for not having a proper Privacy Policy.

☐ Up to **$3.3m** for not disclosing to impacted people that their data has been stolen + additional **$330,000** for not disclosing enough details?

☐ Proposed **removal** of the $3m exception for small businesses.

☐ Would you be interested to reduce your liabilities with the proposed - and existing Australian Privacy Regulations?

4 How do you deliver Breach **Minimisation** today?

☐ Identify, classify, and monitor data and encrypt it as it becomes stale (users can still access).

☐ How do you reduce your attack surface - internal and external to hackers (**not** AV or EDR)?

Quick Breach Cost Estimates

Downtime Costs

Labour Downtime cost ($52k pa = $200/day) $_____/day x __ (qty people) x 10 days = $_____

Lost fixed costs (annual costs / 260) = $_____ daily x 10 days = $_____

Cost of lost revenue (annual income / 260) = $_____

Investigation / Forensics / Recovery

Emergency cost of partner to restore systems (daily cost/person x qty x [10] days) = $_____

Hardware replacement costs - how many & cost of new PC's/servers/devices: $_____

Confidence that the infection has been fully eradicated: ___ / 10

Did hackers / bots manage to steal any Proprietary Intellectual Property?   YES/NO

What is the value/cost if that (IP) becomes generally available to everyone? $_____

Was any money stolen - if so, how much? $_____

Was there a ransomware demand - if so, how much: $_____

Legal / Compliance Costs and Impact

Are you compliant with the NDBS (Notifiable Data Breach Scheme) to notify impacted people

their private data has been stolen (proposed fine up to $3.3m + $330k): $_____

Not having a **proper** Privacy Policy (e.g. secure stale data) $66k or $330k (business):$_____

Defence of lawsuits (lawyers, barristers, judgements, prep time) from being sued: $_____

Invisible Costs

Communicating to clients that they should better protect themselves as their private data has

been stolen, and they may be at risk of a breach, identity theft, and more: $_____

Lost reputation - will you lose any customers (average $/Customer x 3 years): $_____

Negative impact of local media: $_____

Do you have Cyber Insurance - what are the prerequisites of coverage?   YES/NO