INSIGHTS · ISSUE 02

Cyber Risk 101

LOVEDAY INSURANCE SERVICES

A short guide to cyber risk for Australian SMEs and mid-market businesses

Cyber risk refers to the potential for financial loss, operational disruption, or reputational damage resulting from failures in information systems or cyberattacks. For Australian SMEs, the average cost of a cyber incident is approximately $56,000 – and materially higher in severe cases. Most directors are not aware of this figure until after the incident.

The financial impact of an incident

- **Incident response services.** Engagement of a specialist response firm in the first 48 hours typically costs $15,000 to $40,000, even for a contained incident.
- **System recovery and IT remediation.** Forensic investigation, system rebuilding, and restoring data from backups – often the single largest line item.
- **Business interruption.** Lost trading days while systems are down. For revenue-dependent businesses, this can exceed all other categories combined.
- **Legal and regulatory expenses.** Notification costs under the Privacy Act, regulatory engagement, and any subsequent legal proceedings.
- **Reputational damage.** Harder to quantify, but routinely the longest-tail cost. Customer loss, partner caution, and contract delays can extend twelve to twenty-four months beyond the incident.

Five attack types drive most SME incidents.

- **Phishing.** Fraudulent emails designed to extract credentials or trigger payment.
- **Ransomware.** Encrypting systems and demanding payment for their release.
- **Business email compromise (BEC).** Impersonation of suppliers or executives to redirect legitimate payments.
- **Malware.** Software inserted into systems to capture data or disable operations.
- **Identity fraud.** Misuse of personal or business credentials for financial gain.

Phishing and ransomware drive most cyber loss.

Phishing remains the most common entry point for cyber incidents. Attackers use deceptive emails or messages to obtain credentials or trigger fraudulent payment. Ransomware – encrypting business data and demanding payment for its release – is the most damaging single category, with ransom demands rising sharply in recent years.

- **Phishing.** The most common entry point for SME cyber incidents. Attackers exploit familiarity and urgency rather than technical weakness, which is why simple awareness training is more effective than expensive technology in reducing exposure.

- **Ransomware.** The most damaging single category, both financially and operationally. Modern ransomware variants combine data encryption with data theft, so even businesses that have backups face an exposure if the stolen data is published.

Data breaches, BEC and insider threats.

The remaining significant cyber threats to SMEs fall into three groups. Each is meaningfully different from phishing and ransomware in how it operates — and each requires a different category of operational control to manage.

- **Data breaches and privacy.** Exposure of customer or business information can trigger regulatory penalties under the Privacy Act, loss of customer trust, and downstream legal liability. With stricter notification obligations and the prospect of a direct cause of action in privacy law, the consequences of a breach are becoming materially more severe.

- **Business email compromise (BEC).** Attackers impersonate suppliers, executives, or trusted contacts to redirect legitimate payments. BEC exploits trust rather than technical vulnerability, which is why it succeeds against businesses with otherwise reasonable IT controls. It is one of the most under-appreciated SME cyber exposures.

- **Insider threats and human error.** A significant share of cyber incidents are caused by internal factors – employee mistakes, poor password practices, lack of awareness, and inadequate training. Many SMEs do not run regular cyber awareness training, leaving staff unprepared for routine attack patterns.

Third-party risk and the overconfidence gap.

Cyber risk does not stop at the boundary of your own business. The way modern SMEs are connected to suppliers, payment platforms and cloud services means a vulnerability in one provider can quickly become an exposure across many. Layered on top of that is a perception problem – most SME directors believe they are less exposed than they actually are.

- **Third-party and supply chain risk.** Cyber risk arises through IT service providers, payment platforms, cloud applications and other vendors. A vulnerability in one supplier can expose multiple businesses, creating systemic risk that is difficult to insure against and harder to monitor.
- **The overconfidence gap.** A survey of small Australian businesses revealed only 35% feel vulnerable to attack due to being a small business *(Actuaries Institute 2024)*. More than half have already experienced a cyber incident. Many remain unaware of the full range of threats they face – and that gap between perception and reality is itself a meaningful exposure.

"Cyber risk should be treated as a core business risk, not as an IT issue."

How an SME director should think about cyber risk.

Cyber risk should be treated as a core business risk, not as an IT issue. The most common mistake SMEs make is to delegate the question entirely to an IT provider, with the result that the operational controls are reasonable but the board-level oversight is absent. Effective management requires three things.

- **Risk identification.** Understanding which cyber threats are most likely to affect your business specifically. A retail business has a different exposure profile from a professional services firm.
- **Preventative controls.** Implementing baseline measures – multi-factor authentication, current backups, staff training. The Australian Cyber Security Centre's Essential Eight framework is a sensible starting point.
- **Incident response planning.** Knowing in advance who to call in the first 24 hours of a suspected breach. A documented response plan is the single highest-leverage piece of preparation a director can have.

Sources and further reading

The statistics and observations in this guide draw on the following sources. They are listed for readers who want to verify the figures or read further. All sources are publicly available.

AUSTRALIAN CYBER SECURITY CENTRE

Annual Cyber Threat Report.

The Australian government's annual report on cyber threats facing Australian individuals, businesses and critical infrastructure. Source for statistics on incident frequency, attack types, and the prevalence of phishing and ransomware in the SME segment.
https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025

OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER

Notifiable Data Breach Reports.

The OAIC's six-monthly statistical reports on data breaches notified under the Privacy Act. Source for statistics on the categories, frequency and consequences of data breaches affecting Australian organisations.
https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breach-statistics-dashboard

AUSTRALIAN SMALL BUSINESS AND FAMILY ENTERPRISE OMBUDSMAN

Small Business Cyber Resilience Research.

ASBFEO research on Australian small business cyber resilience, including SME owner perception of cyber risk, incident experience, and adoption of baseline controls.
https://asbfeo.gov.au/resources-tools-centre/cyber-security

AUSTRALIAN BUREAU OF STATISTICS

Personal Fraud Survey.

The ABS's periodic survey of Australian experience of identity theft, card fraud and cyber-enabled fraud. Source for statistics on cyber-enabled financial crime and identity-related exposures.
https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release

ACTUARIES INSTITUTE

Cyber protection gap widens for SMEs.

Paper for Actuaries Institute outlining key cyber incidents and the widening gap for cyber risk management between large corporates and SMEs
https://content.actuaries.asn.au/resources/resource-ce6yyqn64sx3-2093352434-54003

Loveday Insurance Services Pty Ltd is a Corporate Authorised Representative (no. 1321366) of McLardy McShane Partners Pty Ltd (AFSL No. 232987) ABN 14 064 465 309
Cyber Risk 101 – Insights · Issue 2 · May 2026.