

Cyber Insurance Insights

March 2026



EBM
Insurance & Risk | Est. 1975



Prepare for a new cyber era

In Australia, a cyber incident is reported on average every six minutes. It's no longer a question of 'if' a business will suffer a cyberattack, but rather 'when'.

With cyber incidents occurring so frequently, the financial impact can be significant. A single cyberattack can cost a business thousands of dollars, making cyber risk a serious and growing concern for businesses of all sizes.

In this environment, understanding the cyber landscape and building an effective protection strategy is essential. One key part of that strategy is cyber insurance, which more businesses are turning to.

In 2025 alone, uptake of cyber insurance increased by 50%, as organisations seek to avoid being caught off guard by growing risks such as ransomware, phishing, social engineering and AI-driven attacks.

Every business is unique, and choosing the right cyber insurance solution can be challenging.

EBM Insurance & Risk is pleased to share insights into the cyber insurance market, to help you make informed decisions and choose the right cover for your business.





Australian Government Targets Ransomware in Cyber Security Strategy

Ransomware is now one of Australia's most pressing cyber threats — and it's hitting businesses hard. In the past five years alone, two thirds of Australian organisations have been caught in its grip. The Australian Signals Directorate (ASD) reports that ransomware made up 11% of all cyber incidents in 2024–25, with its teams responding to 138 attacks — a clear sign that the threat is both widespread and growing.

The Government's 2023–2030 Australian Cyber Security Strategy (ACSS) aims to tackle this growing threat by implementing initiatives that support SMEs and individuals. This includes the release of a ransomware playbook that guides businesses in how to prepare, respond and recover from a ransomware incident.

Mandatory Reporting

While the Government strongly discourages paying ransoms, it has stopped short of an outright ban. However, mandatory reporting of ransomware incidents was implemented by the Australian Government in May 2025 and applies to businesses with annual turnovers of over \$3 million.

'As per section 27 of the Cyber Security Act 2024 (Cth), you have 72 hours to make a ransomware or cyber extortion payment report from the time when you make the ransomware or cyber extortion payment, or from the time you become aware a payment has been made on your behalf.'

Cyber Insurance – A Critical Safety Net

Businesses that invest in cybersecurity and prevention measures are now starting to see more favorable terms become available for their insurance policies. With ransom payments still legal, cyber insurance remains vital with a 2025 McGrathNicol survey finding that 92% of their respondents now have cyber insurance in place.

What Businesses Should Do

- Understand your reporting obligations under the ACSS.
- Review cyber insurance coverage to ensure ransom payments and breach recovery are included.
- Develop a ransomware response plan using the government ransomware playbook as a guide.
- Invest in prevention and detection measures to reduce risk.
- Follow the government's mandatory reporting of ransomware incidents.

With ransomware attacks rising, now is the time for businesses to strengthen their cyber resilience. Talk to your EBM Account Manager about mitigating cyber risks and transferring risk through insurance.



AI adoption among SMEs

Benefits, risks and what businesses need to know

Artificial intelligence (AI) adoption is accelerating across the business landscape, and small-to-medium enterprises (SMEs) are rapidly joining the movement. SMEs are embracing AI or plan to do so, attracted by its potential to drive productivity, profitability, and competitiveness. But alongside the opportunities sit important risks that business owners must manage carefully.

Rapid Growth in AI Adoption

Australia is at the forefront of global AI uptake. Avanade's 2024 AI Readiness Survey found nearly 80% of Australian businesses use AI daily—well above the global average of 57%. Nearly all believe they must transition to an AI first model within the next year to remain competitive.

SMEs are also investing. NAB's SME Business Insights report shows 23% have already dedicated time or money to AI, machine learning or automation, while another 20% plan to. Their expectations are high: four in ten SMEs hope AI will increase profitability, and six in ten expect productivity gains.

Benefits Driving SME Investment

Productivity improvements and reduced administrative workloads are the major drawcards. NAB reports that about 40% of SMEs expect AI to boost profits, while one third believe AI will improve handling of customer queries.

Commonwealth Bank research supports this trend: 87% of SMEs using AI report cost and time savings, and more than half say it has contributed to business growth. Popular applications include content creation, idea generation, and automation of routine tasks.

Emerging Risks for SMEs

Despite strong demand, many SMEs remain cautious. Statista data shows high public concern around AI scams, deepfakes, data privacy and bias. For businesses, key risks include cybersecurity threats, poor data quality, ethical challenges, and potential job impacts.

Security is the most pressing issue. Studies from Absolute Security, Palo Alto, Darktrace and others show many organisations feel underprepared for AI powered cyberattacks, which are becoming increasingly sophisticated. Criminals are using AI to create adaptive malware, automate attacks, and elevate phishing campaigns. Cloud security is also a concern, especially where misconfigurations or leaked credentials provide entry points for attackers.

Data integrity is another critical risk. Because AI relies on vast datasets, businesses must safeguard sensitive information and understand how platforms store and use uploaded content. Accuracy is an issue too—AI models can generate low quality, outdated or incorrect information, with some models known to “hallucinate” fabricated facts.

The rise of highly convincing AI-generated content also raises ethical and reputational risks, as it becomes harder for audiences to distinguish real from artificial material.

Managing AI Risks

To safely capture the benefits of AI, SMEs need strong governance and risk management frameworks. Key actions include:

- Understanding relevant data protection and privacy requirements
- Implementing clear internal AI-use policies
- Modernising IT systems and strengthening cybersecurity controls
- Ensuring secure data storage and access management
- Testing AI tools for accuracy, ethics, and reliability
- Training employees in safe and effective AI use
- Maintaining human oversight over AI-generated outputs.



The Cybersecurity threat of Australia's rapid drone expansion

Commercial drone use in Australia is rising at an extraordinary rate. What was once futuristic technology is now an everyday sight, with drones being used across industries for tasks ranging from surveying and environmental monitoring to food delivery and emergency response. While the technology brings efficiency, speed and new commercial opportunities, it also introduces significant cybersecurity risks that businesses must be prepared for.

A Rapidly Growing Industry

Drones are now integral to sectors including agriculture, mining, construction, logistics, and coastal surveillance. Globally, the drone market is expected to reach US\$67.64 billion by 2029, with production increasing from two million units in 2021 to 6.5 million by 2030.

It is expected that drones will play a major role in everyday operations across the country. Projections include over 3.5 million environmental monitoring flights, nearly 500,000 agricultural flights, 500,000 medical deliveries, and 1.5 million food deliveries each year.

Mining operations are expected to conduct almost half a million drone flights annually, while policing will rely on more than 300,000. Goods delivery will dominate, reaching 46 million flights a year and accounting for 77% of all drone activity.

Passenger drone transport will also emerge, with close to one million such flights forecast annually by 2043, including the movement of approximately 100,000 patients.

Why Cybercriminals Target Drones

As drone capabilities evolve—flying farther, faster and gathering increasingly detailed data—their value to cybercriminals increases. Drones rely on wireless communication technologies such as GPS, Wi-Fi, Bluetooth and radio frequency. These systems are highly vulnerable to interception, manipulation and unauthorised access, especially because drones are operated remotely.

Cyber attackers can hijack drones, intercept transmitted video or data, or use the device as a launch point to infiltrate corporate networks. In many cases, criminals do not even need their own drone—they can hack into an existing one and repurpose it.

Examples of major attack types include:

- GPS spoofing: feeding a drone false coordinates to redirect or crash it.
- Command and control interception: taking full control of the drone by hijacking the communication link.
- Downlink interception: capturing data being transmitted to the operator.
- Distributed Denial of Service (DDoS) attacks: overwhelming the drone's communication channels and causing loss of control.
- Signal jamming: disrupting the connection between the drone and its base station.
- Data exploitation: using drone mounted devices to mimic Wi-Fi networks, steal passwords, or hijack Bluetooth peripherals.

Mitigating the Risk

- Use VPNs to encrypt drone communications
- Enforce strong authentication and access controls
- Update firmware and apply patches promptly
- Secure controller devices with antivirus software
- Use strong, unique passwords
- Limit device connections to the base station
- Ensure drones have a reliable Return to Home function
- Secure networks, especially IoT devices, and avoid default credentials.

Insurance also plays a crucial role. Cyber insurance—and specific drone coverage—can help protect against operational and financial losses.

The rising risk of Cyberwashing

Why exaggerating Cybersecurity can backfire

As cyber threats escalate globally, businesses of all sizes are increasingly concerned about their vulnerability to attacks. Recent research highlights the scale of the issue: Cyber Warden's 2024 Pulse Check found that 82% of Australian small businesses fear cyberattacks, and the same percentage experienced an incident in the past year. Globally, the Allianz Risk Barometer 2025 reports that cyber incidents remain the number one business risk for the fourth consecutive year. With three quarters of Australian organisations expecting a breach in 2025, cybersecurity has never been more critical.

In response, many organisations are investing heavily in security measures. Gartner predicts global cybersecurity spending will rise to US\$239 billion in 2026. However, alongside legitimate improvements, a troubling trend has emerged—cyberwashing, where organisations exaggerate or misrepresent their cybersecurity capabilities to appear more secure than they truly are.

What Is Cyberwashing?

Cyberwashing involves misleading claims about cybersecurity practices, data handling standards, or incident response capabilities. It also includes downplaying the cause or severity of a breach or overstating how effectively it was managed.

A Monash University report warns that cyberwashing is becoming increasingly common. Lead researcher Professor Nigel Phair highlights a growing gap between what companies say and what they actually do. High profile breaches at Optus, Medibank and Latitude Financial underscore this disconnect, with organisations initially claiming strong cybersecurity controls before investigations revealed significant weaknesses. Cyberwashing, Phair notes, erodes trust and increases financial, reputational, and legal risks.

Regulators Put Cyberwashing Under the Microscope

Australia's corporate regulator, ASIC, is taking cybersecurity failings seriously. It considers cybersecurity a core part of directors' duties, viewing inadequate cyber preparedness as a foreseeable risk. ASIC have warned boards that failure to prioritise cyber resilience may lead to enforcement action.

In 2025, ASIC named "inadequate cybersecurity protections" as a key enforcement priority. It has already taken legal action against FIIG Securities, alleging the company failed to maintain sufficient cyber risk management systems, enabling a hacker to remain undetected for 20 days. This follows ASIC's landmark case against RI Advice in 2022, where the court ruled the company breached its licence obligations after multiple cyber incidents exposed thousands of client files.

ASIC Commissioner Simone Constant has explicitly linked this enforcement agenda to cyberwashing, stating that organisations must have evidence to support cybersecurity claims. "We don't want to see the rise of cyberwashing," she said.

Cyberwashing and Class Action Liability

Cyberwashing is also emerging as a major theme in data breach litigation. Class actions against Optus and Medibank allege the companies misrepresented their security posture in privacy policies and communications with customers. As law firm Allens notes, the central theme in these cases is the allegation that companies made promises about their cybersecurity standards that were ultimately untrue.

Insurance Implications: A Hidden but Major Risk

Cyberwashing can also jeopardise insurance cover. Cyber insurance applications require accurate disclosure of security controls. If a business misrepresents its cybersecurity posture—whether deliberately or through misunderstanding—insurers may deny claims, reduce payouts, or void policies entirely. This risk can also extend to other policies, such as Directors & Officers (D&O) insurance, where cybersecurity is now a key underwriting factor.

Insurers are increasingly acting as a check on cyberwashing. If a business is found not to have maintained the level of security stated in their proposal, cover may be denied.

Reducing the Risk

To protect the business, organisations should ensure all cybersecurity statements—whether in policies, marketing materials, compliance documents or insurance proposals—accurately reflect reality.

Data breaches hit record levels

What businesses need to know

Data breaches reached unprecedented levels in 2024, and the threat shows no sign of slowing. From retailers and universities to government agencies and major corporations, hardly a day goes by without news of another cyber incident. The Qantas breach, which exposed personal details of approximately six million customers, is a stark reminder of the growing risk. While financial and passport details were not compromised, the attack highlights how vulnerable organisations remain.

Record-Breaking Breach Notifications

The Office of the Australian Information Commissioner (OAIC) reported 532 notifiable data breaches in the January-June 2025 reporting period. Under the Notifiable Data Breaches (NDB) scheme, organisations covered by the Privacy Act 1988 must report breaches likely to cause serious harm. Yet, these figures only scratch the surface—many incidents go unreported.

What's Driving the Surge?

Malicious and criminal attacks accounted for 69% of all notifiable data breaches in the second half of 2024, with phishing, ransomware, and credential theft leading the charge. Social engineering attacks rose sharply, making up 28% of malicious breaches, while insider threats contributed 7%. Human error remains a significant factor, responsible for 29% of breaches, often due to misdirected emails or failure to use Blind Carbon Copy (BCC). Health services, government agencies, and financial institutions were the hardest hit sectors.

Penalties for serious or repeated data breaches

Australian Privacy Regulations have increasingly higher standards and penalties. Maximum penalties can be applied for serious or repeated privacy breaches under the Privacy Act 1988 by a body corporate, with the penalty being the greater of:

- \$50 million
- Three times the value of any benefit obtained through the misuse of information, or
- 30% of the body corporate's adjusted turnover during the breach turnover period, if the benefit cannot be determined.

How Businesses Can Respond

With cybercrime reported every six minutes in Australia, organisations must act decisively. Key steps include:

- Understand obligations under the NDB scheme and Privacy Act 1988.
- Limit data collection to what's necessary and implement strict access controls.
- Secure storage and disposal of personal information, both physical and digital.
- Train employees on privacy and cybersecurity best practices.
- Maintain strong cyber hygiene: update software, enforce strong passwords, enable multifactor authentication, encrypt data, and conduct regular security audits.
- Prepare an incident response plan for quick detection, notification, and recovery.
- Consider cyber insurance to mitigate financial risk.

The message is clear: data protection is no longer optional - it's a business imperative.

Consider a Cyber Insurance policy; it is designed to protect your business against the expenses and legal costs associated with data breaches.

How businesses can protect themselves from human-focused cyberattacks

As cybercriminals increasingly target human vulnerabilities rather than technical weaknesses, businesses face growing pressure to strengthen defences that protect staff, systems and data.

What Is Social Engineering?

Social engineering involves manipulating individuals into divulging sensitive information, performing unauthorised actions, or bypassing established security procedures. Rather than “hacking” through technical barriers, cybercriminals exploit psychological triggers such as trust, authority, empathy and urgency.

According to the Office of the Australian Information Commissioner (OAIC), 28% of malicious breaches in the second half of 2024 involved social engineering or impersonation. The rise of AI enhanced deception—through voice cloning, deepfakes and automated interaction—has made these attacks increasingly sophisticated.

Common tactics include phishing, spear phishing, vishing (phone scams), pretexting, business email compromise, baiting, and impersonation of executives or trusted vendors. Once criminals obtain access or information, they may commit identity theft, install ransomware, redirect payments, or exfiltrate sensitive data.

How Social Engineering Attacks Unfold

Most social engineering campaigns follow a predictable pattern:

1. Research – gathering details about staff, systems and processes
2. Pretexting – creating a believable scenario or identity
3. Execution – contacting the target, often using urgency or fear
4. Exploitation – extracting data, access or money
5. Capitalisation – committing fraud, extortion or data theft
6. Cover up – hiding tracks by deleting logs or masking behaviour

Individuals most frequently targeted include executives, administrators, finance staff, HR, IT help desks, and employees regularly dealing with external contacts.

Why Social Engineering Fraud Is So Costly

Social engineering fraud (SEF) is now one of the most common—and financially damaging—forms of cybercrime.

With AI making impersonation easier and more convincing, SEF has grown from crude phishing emails to highly tailored schemes involving live interaction, synthetic voices, deepfaked video and multichannel deception.

Insurance Implications

Coverage for SEF varies significantly across cyber and crime insurance policies. Some cyber policies exclude SEF entirely, while crime/fidelity policies may only cover “direct” fraud, not losses caused by manipulation. Endorsements or sub-limits may apply, making accurate disclosure of cybersecurity practices critical. Misrepresentation of controls during underwriting can jeopardise claims.

Reducing the Risk

Businesses can strengthen defences by:

- Training staff to recognise manipulation and suspicious communications
- Implementing strong security policies and access controls
- Using MFA (multi-factor authentication), password management tools and device security
- Verifying requests—especially involving money or sensitive data—via independent channels
- Deploying email filtering, URL scanning and intrusion detection tools
- Using zero-trust security models and limiting employee access
- Conducting regular audits, monitoring logs, and reviewing third party security.

Key Takeaway

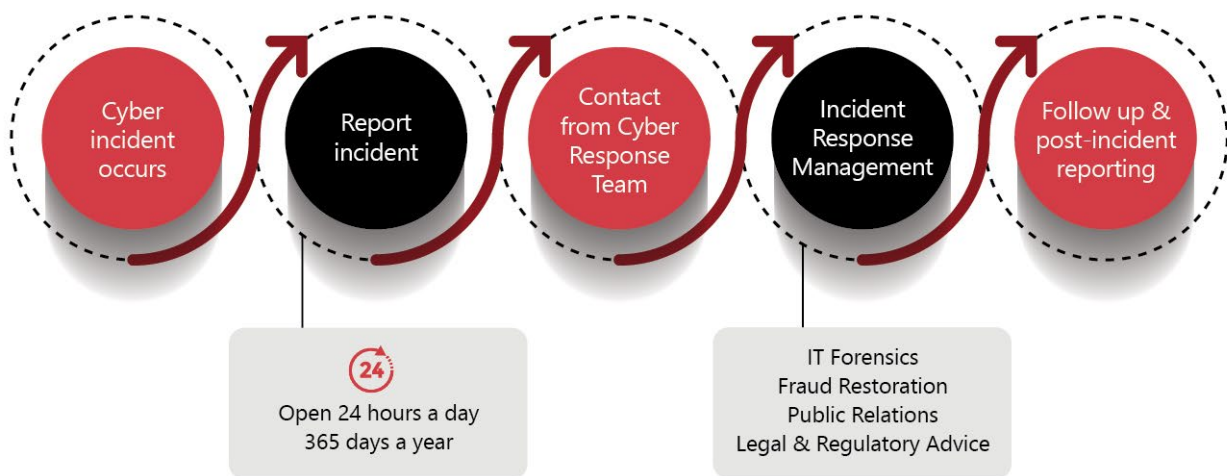
Social engineering is one of the most significant cybersecurity threats facing Australian businesses. While technical controls are essential, human-centred security awareness and strong processes remain the most effective defence.



What can a typical Cyber Incident Response Plan look like?

Cyber Incident Response Services can help your business:

- Act quickly to contain the threat and limit potential damage to your business
- Meet the obligations under the Privacy Act
- Limit the consequences of a data breach
- Preserve and maintain public trust.



*The above workflow diagram is an example only.

Cyber Insurance policies are designed to cover response and recovery expenses (not just data compromise) and generally include:

- Incident response and investigation costs
- Crisis management support via 24-hour incident reporting hotline
- Legal costs in defense and investigation
- Regulatory fines, penalties and defense costs.

Talk to your EBM Account Manager about mitigating cyber risks and transferring risk through insurance.





EBM
Insurance & Risk | Est. 1975

P: 1300 755 112

ebm@ebm.com.au ebm.com.au

Elkington Bishop Molineaux Insurance Brokers Pty Ltd
AFSLN 246986 | ABN 31 009 179 640

[New South Wales](#) [Victoria](#) [Queensland](#) [Western Australia](#) [South Australia](#)

[National Insurance Brokers Association](#) | [Coverholder at Lloyd's](#) | [Asia Australasia Alliance](#) | [GBN Worldwide](#) | [Worldwide Broker Network](#)