EmergeIT

Australia's Cyber Wake-Up Call: Key Insights from the 2024–25 ASD Threat Report for Business Leaders

Introduction – The State of Cyber Risk in Australia

Australia's economy has become one of the most digitally connected in the world, and this brings both opportunity and exposure. The Australian Signals Directorate's (ASD's) *Annual Cyber Threat Report 2024–25* shows that our growing reliance on online systems continues to attract criminal and state-sponsored actors alike.

Over the past twelve months, cyber incidents and financial losses have again risen. The Australian Cyber Security Centre (ACSC), part of the ASD, received approximately 42,500 calls to the national Cyber Security Hotline, a 16 per cent increase, and responded to over 1,200 significant cyber incidents, up 11 per cent. Meanwhile, around 84,700 cybercrime reports were lodged through ReportCyber, which is an average of one every six minutes.

For Australian businesses, responding to cybercrime has become a cost of doing business. The same tactics once reserved for government or critical-infrastructure targets are now routinely used against private enterprises, especially those in the small-to-medium sector.

Cybercrime Is Now Big Business

The ASD's report paints a clear picture of a thriving professional cybercrime economy. Cybercriminals have industrialised their operations, selling stolen data, malicious software, and network access to others through online marketplaces. The rise of "cybercrime-as-a-service" has lowered the barrier to entry, allowing even low-skill offenders to rent or buy ready-made attack tools.

Ransomware remains one of the most damaging forms of cybercrime. These attacks encrypt data, disrupt operations, and demand payment for restoration. Increasingly, ransomware is coupled with data theft, known as "double extortion", where attackers threaten to publish stolen files if their demands aren't met.

Another growing threat is information stealer malware, a class of malicious software designed to harvest usernames, passwords, credit-card details, and browser data. Stolen credentials are then resold on criminal marketplaces, providing a steady supply of access points into Australian organisations.

This commoditised approach to hacking has created a self-sustaining ecosystem where one attacker's success becomes another's starting point. For legitimate businesses, it means exposure can occur long after an initial breach has been forgotten.

Counting the Cost – The Numbers Behind the Threat

Cybercrime's financial impact is accelerating across every business category. The ASD's latest report shows that while larger organisations bear the biggest absolute losses, smaller firms are no longer insulated from serious financial harm.

Business Size	Typical Characteristics	Average Cost per Incident (FY 2024–25)	Year-on-Year Change
Small	Fewer than 20 employees, turnover < $10 million	$56,600	↑ 14 %
Medium	20 – 199 employees, turnover $10 – $100 million	$97,200	↑ 55 %
Large	200+ employees, turnover > $100 million	$202,700	↑ 219 %

The same attack patterns that cripple multinational corporations are now scaled down and automated against smaller targets with fewer defences.

Identity fraud, business email compromise, and invoice redirection fraud continue to be the leading causes of loss. However, attackers increasingly rely on psychological manipulation (creating urgency, exploiting trust, or impersonating suppliers) to trick victims into transferring money or divulging credentials.

These trends show that the financial and reputational damage of a single cyber incident can easily exceed years of incremental IT investment.

How Attacks Typically Begin

Most cyber incidents still begin with simple but effective techniques that exploit human behaviour or outdated technology.

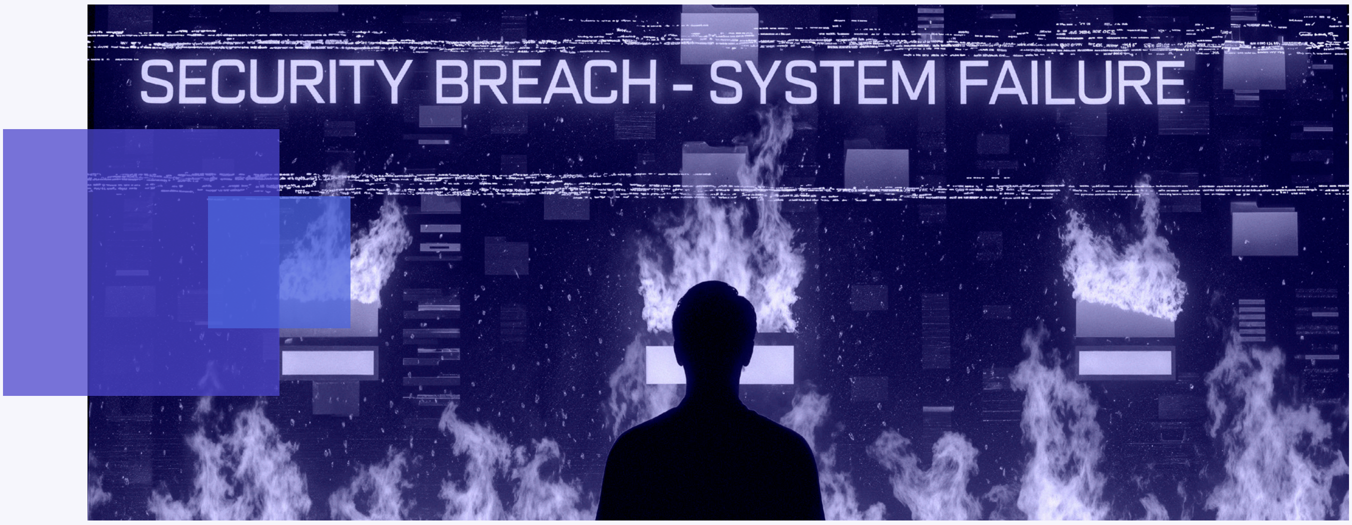
Phishing and social engineering remain the dominant entry points, accounting for 38 per cent of incidents. Attackers craft convincing messages, often using stolen data or publicly available details, to persuade employees to click links, open attachments, or reveal credentials. AI tools are now being used to refine these messages, making them grammatically flawless, well branded, and highly targeted.

Stolen or reused credentials are another common weakness. Passwords compromised in previous data breaches are purchased in bulk on the dark web and used to log in directly to business systems. In many cases, the attackers never need to "hack" anything; they simply exploit the absence of multi-factor authentication.

Unpatched systems and devices provide another easy route in. Vulnerabilities in routers, firewalls, and outdated applications are widely published online, and attackers can use automated scanning tools to locate exploitable systems within hours of disclosure.

Business email compromise scams continue to evolve. Criminals infiltrate legitimate email threads, alter invoice details, and redirect payments to offshore accounts. These scams are increasingly supported by AI-generated identities and fraudulent documentation, making them difficult to detect through casual review.

Ultimately, most incidents still exploit predictable weaknesses, human error, weak authentication, and neglected maintenance, rather than advanced technical skill.



The SME Risk Profile – Why Smaller Targets Are Attractive

Small and medium-sized enterprises have become a favoured target precisely because they sit at the intersection of value and vulnerability. They hold valuable data such as client records, financial information, and intellectual property, yet often lack the resources to defend it comprehensively.

The ASD notes that many smaller businesses:

- Rely on shared or reused passwords across multiple systems
- Outsource IT support only without clear accountability for security outcomes
- Use outdated network hardware, such as routers and VPN devices
- Have limited visibility into what’s happening on their networks

All of this creates an environment where attackers can easily gain a foothold, move laterally, and exploit trusted business relationships. In some cases, compromising a small contractor provides indirect access to a larger partner’s systems, making SMEs a gateway for broader attacks.

The shift to hybrid and remote work has only increased exposure. Personal mobiles and laptops, home Wi-Fi routers, and cloud applications are now part of the corporate attack surface. The ASD observed that 96 per cent of attacks on “edge devices”, such as routers and firewalls, were successful. These devices often operate with default passwords or outdated firmware, turning them into silent entry points.

Emerging Trends to Watch

Artificial Intelligence in the Hands of Attackers

The Cyber Threat Report highlights the dual nature of AI in cybersecurity. While businesses explore generative-AI tools to improve efficiency, cybercriminals use the same technology to enhance deception and scale attacks. AI can:

- draft convincing phishing messages in seconds;
- generate fake identities, voices, and documents; and
- analyse stolen data faster to extract valuable targets.

As AI models become more accessible, the time between data theft and exploitation is shrinking, leaving victims less opportunity to respond.

Data Theft and Multi-Stage Extortion

Criminal groups increasingly use stolen data for multiple revenue streams. A single breach may lead to ransom demands, sale of data on the dark web, identity theft, and follow-on fraud against clients or suppliers. Victims often face legal and reputational fallout long after paying for remediation.

Legacy IT and Technical Debt

Old hardware and unsupported software remain a recurring weakness. Legacy systems, although they often host critical business data, are difficult to patch, making them an ideal entry point. The cost of replacing outdated technology may seem high, but the numbers show that remediation after compromise is consistently more expensive.

Disruption Over Destruction

Denial-of-service (DoS and DDoS) attacks increased by 280 per cent in the past year. The increase was attributed to the increasing availability of botnet rental services and automated attack platforms, which enable threat actors to launch high-volume traffic floods at lower cost and with minimal technical overhead, increasingly allowing them to target smaller businesses.

While these events rarely cause permanent damage, they disrupt online services and divert resources from core operations. For smaller firms that rely on e-commerce or cloud platforms, the ASD notes that even brief outages can have measurable financial consequences.

Practical Resilience – What Works

In its report, the ASD reinforces that the majority of incidents it investigates could have been prevented through a handful of well-implemented fundamentals such as:

1 Enable phishing-resistant multi-factor authentication

SMS-based codes offer limited protection and are susceptible to interception. Instead, use passkeys or authenticator apps for email, finance, and admin systems.

2 Keep devices and software updated

Apply updates as soon as possible, particularly for internet-facing systems like routers and VPNs. Replace products no longer supported by the manufacturer.

3 Use strong, unique passwords and manage them securely

Implement a reputable password manager to generate and store unique credentials for every service. Avoid reusing passwords across accounts.

4 Back up business-critical data

Maintain offline or cloud-based backups and conduct recovery tests. Regular testing ensures backups remain viable during a crisis.

5 Know who manages what

If using an external IT provider or managed service, clarify who’s responsible for patching, monitoring, and incident response. Document these expectations contractually.

6 Retire legacy IT systems

Replace or isolate unsupported technology. Short-term workarounds, such as network segmentation, can reduce but not eliminate the risk.

7 Monitor and log network activity

Basic logging tools or managed-detection services help identify suspicious access early, reducing incident duration and cost.

8 Prepare and rehearse an incident-response plan

Know who to contact, how to isolate affected systems, and how to communicate with clients. The ACSC provides free guidance through cyber.gov.au and its 24/7 hotline (1300 CYBER1).

These steps align with ASD’s Essential Eight mitigation strategies, a practical framework designed to protect organisations from the most common forms of attack.

Shifting the Mindset – From "It Won't Happen to Us" to "Assume Compromise"

The ASD encourages all organisations to adopt an assume-breach mindset, accepting that a cyber incident is not a matter of if, but when. This shift changes the question from "How do we prevent every attack?" to "How do we limit damage and recover quickly?"

For SMEs, this means identifying the digital "crown jewels": for example,

(1) customer databases; (2) financial systems including invoicing, payroll and banking access; (3) proprietary designs, trade secrets or intellectual property; and (4) access credentials for cloud services and business-critical applications. Prioritising the protection of these assets helps ensure that limited resources are applied where they deliver the greatest risk reduction.

Cybersecurity should also be embedded in governance. Just as financial controls and workplace safety have specific people accountable for them, information security warrants board-level oversight. Regular reporting on patch status, incident logs, and supplier compliance helps ensure that security is treated as a measurable business outcome rather than a technical afterthought.

Perhaps most important, however, is education. Employees are both the first line of defence and, unintentionally, the most common point of failure. Periodic awareness training, focused on recognising scams, verifying requests for payment changes, and handling sensitive information, reduces the likelihood of human error leading to compromise.

A strong security culture is not about fear; it's about readiness. Businesses that normalise basic protective habits are far more resilient when incidents occur.

Government and Industry Collaboration

The good news for small businesses is that there's growing cooperation between government, law enforcement, and private industry to disrupt cybercriminal infrastructure. Initiatives such as **Operation Aquila**, a joint effort between the ASD and the Australian Federal Police, have successfully targeted ransomware groups and taken down servers hosting stolen data.

The government has also introduced a **mandatory ransomware-reporting regime** for businesses with annual turnovers above $3 million. While this won't apply to most SMEs, the requirement signals an increasing expectation for transparency and data stewardship across the economy.

Over **133,000 organisations** now participate in the ACSC's Cyber Security Partnership Program, receiving alerts, technical guidance, and training opportunities. The ACSC also conducts national cyber drills in which teams simulate attacks in controlled environments, an initiative that underscores the importance of practising response, not just prevention.

These efforts indicate a shift toward a **collective defence model**, where public and private sectors share intelligence and coordinate action to protect Australia's digital ecosystem.

Turning Awareness into Action

The 2024–25 ASD report makes it clear that cybercrime is an enduring challenge rather than a temporary wave. The volume of attacks continues to rise, but so too does the availability of guidance, tools, and frameworks to counter them.

For SMEs, the implications are straightforward: cybersecurity is now a fundamental component of business continuity and reputation management. A single incident can disrupt operations, erode customer trust, and trigger regulatory scrutiny. Yet, most attacks succeed not because they're sophisticated, but because the target's defences are incomplete or inconsistent.

Building resilience doesn't require enterprise-level budgets. It takes consistent application of the basics, multi-factor authentication, timely updates, regular backups, and an informed workforce. The ASD's findings reaffirm that these measures alone could have prevented the majority of incidents reported last year.

Australia's economic strength depends more and more on the digital integrity of its small-business community. Awareness is no longer optional, and action cannot wait. By embedding cyber awareness into everyday practice, SMEs can transform from easy targets into resilient participants in the nation's digital future.

Emerge IT

Contact info

☎ 1300 348 287

✉ hello@emergeit.com.au

🌐 www.linkedin.com/company/emerge-it-solutions-pty-ltd