Australia's Cybersecurity Crisis: It's Time to Act

The alarm bells are ringing loud, and they're impossible to ignore. Over the past three years, Australia has experienced a watershed moment in cybersecurity—one that demands immediate action from every medium and large organization in the country.

The Reality Check: Major Breaches That Shook the Nation

The numbers tell a sobering story. Over 1,100 data breaches were reported in Australia in 2024, a 25% jump from 2023, with cyber security incidents accounting for the majority. But the headline-grabbing incidents reveal just how vulnerable even our largest corporations remain.

The Major Incidents - 2024 to 2026:

Finance & Travel Sector:

- **Qantas (June 2025)**: Australia's largest airline experienced a significant data breach potentially impacting up to 6 million customers through a sophisticated social engineering attack targeting its Manila-based call center, highlighting vulnerabilities in outsourced operations.
- **Hertz, Dollar & Thrifty (October-December 2024, Disclosed April 2025)**: The rental car companies notified customers after confirming that a file-transfer vendor, Cleo Communications, suffered a cyberattack between October and December 2024. Exposed data included names, contact details, dates of birth, driver license details, with some records containing Tax File Numbers, passport data, and payment card information. The breach was linked to the Clop ransomware group.
- **Zurich Insurance Group (March 2025)**: A threat actor claimed access to 1,400+ internal files and began sharing samples on cybercrime forums in early March 2025.
- **Austin's Financial Solutions**: Kairos ransomware group claimed responsibility for hacking this NSW wealth management firm, stealing and publishing 147 gigabytes of data.

Healthcare & Pharmaceuticals:

- **DBG Health (August 2024, Disclosed January 2025)**: The Morpheus ransomware group claimed responsibility for an intrusion detected on August 25, 2024. Nearly 2.5 TB of stolen data was exposed, including patient-related records, employee information,

and internal business material such as payroll and confidential documents.

Retail & Consumer:

- **Early Settler (August 2024)**: The well-known Australian furniture and home goods retailer experienced a significant data breach that exposed the personal information of 1.1 million customers.
- **Fullerton Hotels and Resorts (2024)**: Hackers obtained a 148-gigabyte data breach from the luxury Sydney hotel, including passports and driver licences.

Telecommunications:

- **Tangerine Telecom (February 2024)**: The popular Australian telecommunications provider experienced a data breach exposing the personal information of 232,000 customers, including full names, dates of birth, mobile numbers, email addresses, postal addresses, and account numbers.
- **Telstra (April 2024)**: One of Australia's largest telecommunications providers disclosed a data breach exposing the personal information of approximately 47,000 customers, including names, email addresses, and phone numbers.

Education & Public Sector:

- **Western Sydney University (July 2024, Disclosed 2025)**: Around 10,000 students were impacted by unauthorized access to the university's systems. A 27-year-old former student was charged with 21 offences after allegedly hacking the system over a four-year period, accessing it for free parking, changing grades, and downloading over 100GB of personal information.
- **Copyright Agency (2024-2025)**: Notified 37,000-plus members after investigating a cyber incident.

Other Notable Incidents (2024-2025):

- **Clubs NSW (May 2024)**: The peak body representing registered clubs in New South Wales suffered a data breach compromising the personal information of approximately 1 million members.
- **Globelink International (December 2024)**: The Qilin ransomware operation claimed responsibility, stealing almost 30,000 files from this Australian freight forwarder.
- **REST & AustralianSuper (2025)**: Major superannuation funds were targets of what appears to be a coordinated cybersecurity attack on the industry, affecting member accounts.
- **Novati (2024)**: The Lynx ransomware group targeted this Sydney-based construction

company, stealing records of contracts, financial data, and incidents.

The Escalating Threat Landscape

The trajectory is deeply concerning and accelerating. Over 1,100 data breaches were reported in Australia in 2024, a 25% jump from 2023. The volume and cost of breaches continue to rise dramatically.

Key Statistics (2024-2025):

- The OAIC received 595 data breach notifications between July and December 2024, an increase of 15% compared to the previous 6 months
- In the January–June 2025 reporting period the average number of individuals affected by cyber incidents is just over 10,000
- IBM calculates that in 2024 the average cost to business of a data breach was $4.26 million
- ASD's ACSC responded to over 1,200 cyber security incidents, an 11% increase, and notified entities more than 1,700 times of potentially malicious cyber activity – an 83% increase from the previous year
- DDoS or denial-of-service incidents increased by 280%

Sector-Specific Vulnerabilities:

The health sector had the most reported data breaches (18% of reported data breaches) with the finance sector reporting the second greatest number (14%), followed by Australian Government agencies (13%).

Attack Methods Are Evolving:

- In January–June 2025, human error accounted for 37% of all data breaches (193 notifications), an increase from 29% in the previous reporting period
- Around 46% of confirmed incidents in 2024 were related to malware and ransomware attacks
- Malicious attacks accounted for 69% of reported breaches in the 6 months to December 2024
- Social engineering attacks targeting call centers have become highly sophisticated, as evidenced by the Qantas breach
- State-sponsored cyber actors continue to pose a serious and growing threat to our nation, targeting networks operated by Australian governments, critical infrastructure

and businesses

What Medium and Large Companies Must Do NOW

The time for incremental improvements has passed. Here's what organizations need to prioritize:

1. Implement Zero-Trust Architecture

Stop assuming anything inside your network is trustworthy. Every access request—whether from employees, contractors, or systems—must be verified. This is no longer optional.

2. Mandate Multi-Factor Authentication (MFA) Everywhere

Credential stuffing attacks have become increasingly effective when passwords are reused across multiple accounts. MFA is your first line of defense. Make it non-negotiable for all employees and, critically, for all access to sensitive systems.

3. Develop a Robust Incident Response Plan

You need:

- A documented incident response playbook tested through regular tabletop exercises
- A designated incident response team with clear roles and responsibilities
- Clear communication protocols for breach notification (you'll need to comply with mandatory reporting requirements)
- Partnerships with external response resources and forensics firms

4. Strengthen Your Third-Party Risk Management

Third-party systems widen the attack surface, with outsourcing to third parties highlighted as a source of exposure.

Create a vendor security assessment program that includes:

- Regular security audits of critical vendors
- Contractual requirements for cybersecurity standards
- Data handling agreements that specify how your information is protected
- Supply chain visibility and monitoring

5. Invest in Employee Security Training

Human error remains a significant factor in data breaches, with phishing and social engineering being primary entry points. Monthly security awareness training—not just annual checkbox compliance—is essential.

6. Establish a Data Governance Framework

Know what data you hold, where it's stored, who has access, and how long you keep it. Implement:

- Data classification systems
- Purpose-driven data minimization
- Regular data audits
- Clear retention and disposal policies

7. Prioritize Ransomware Preparedness

- Regular backup testing (offline backups, not connected to your network)
- Ransomware-specific tabletop exercises
- Clarity on your organization's position regarding ransom payments
- Awareness that as of May 2025, a mandatory ransomware reporting regime for businesses with annual turnovers of $3 million or more has been introduced

8. Conduct Penetration Testing and Vulnerability Assessments

Partner with qualified security professionals to stress-test your defenses regularly. It's far cheaper to find vulnerabilities yourself than through a breach.

9. Monitor and Detect Threats Actively

Implement Security Information and Event Management (SIEM) and threat detection tools. Passive security is not enough—you need active monitoring, threat hunting, and 24/7 security operations capability.

10. Align with Regulatory Requirements

Stay informed about:

- Updated Privacy Act requirements
- Notifiable Data Breaches scheme obligations
- Industry-specific standards relevant to your sector

- The upcoming Security of Critical Infrastructure Act implications

The Bottom Line

Australia's cybersecurity landscape has fundamentally shifted. The breaches of the past three years aren't anomalies—they're a preview of the new normal. The organizations that survive and thrive are those that treat cybersecurity as a business-critical function with executive accountability and adequate investment.

Your data—and your customers' data—is your responsibility. The reputational damage, financial penalties, and operational disruption from a breach far exceed the cost of getting your security posture right today.

The question isn't whether you'll face a cyber threat. It's whether you'll be ready when you do.

References:

- Australian Signals Directorate Annual Cyber Threat Reports (2023-2024, 2024-2025)
- Office of the Australian Information Commissioner (OAIC) Notifiable Data Breaches Scheme
- ASD Australian Cyber Security Centre (ACSC) Data
- Multiple breach reporting sources and industry analyses (2023-2025)