WHITE PAPER

Australia's cyber leap: A bold cyber security strategy to spur business and innovation

protiviti®
Global Business Consulting

Introduction

For boards and executives in Australia, cybersecurity obligations now carry a weight comparable to financial reporting and workplace safety. An ambitious, nationwide cybersecurity reform calls on businesses and government entities to demonstrate due diligence, proactive governance, and timely reporting that are no longer optional — they are regulatory imperatives set in place by the Australian government though its 2023-2030 Cyber Security Strategy.

Sweeping reforms like this generate excitement and opportunities for businesses while posing new complexities and challenges. Organisations face framework overlap, resource pressures, persistent skills shortages, rising insurance exclusions, and systemic supply chain vulnerabilities. To navigate this environment, businesses require a comprehensive understanding of not only the reforms as a whole but also their sector-specific implications. In this paper, we offer our analysis of the regulatory cybersecurity landscape and highlight challenges and opportunities for key industries in Australia.

The strategic context: Australia's 2023-2030 cyber security strategy

Australia is currently at a critical stage in its cybersecurity journey. The 2022–2023 data breach wave, which exposed the confidential information of millions of Australians in the telecommunications, healthcare, financial services, and retail sectors, served as a wake-up call for both government and industry. In response, the Australian government implemented the 2023–2030 Australian Cyber Security Strategy, which is supported by $586.9 million in funding, regulatory reforms, and an ambitious objective to establish Australia as a world leader in cyber security by 2030 (Department of Home Affairs, 2023).

The goal of this cybersecurity reform is not merely to mitigate threats; it is also to redefine the way in which organisations operate, transfer accountability to the boardroom, and reshape industries. It is imperative for administrators and decision-makers to comprehend these changes to safeguard trust, maintain competitiveness and facilitate digital transformation.

We are shifting cyber from a technical topic to whole-of-nation endeavour, focusing on providing better support to civilians and industry.

Source: Department of Home Affairs

A joint effort to build nationwide resilience

The 2023-2030 Australian Cyber Security Strategy impacts both public and private organisations, leveraging cybersecurity as a strategic enabler for growth, trust and resilience nationwide.

The strategy introduces six "cyber shields": enhanced businesses and citizens, secure technology, world-class threat sharing, sovereign capability development, international partnerships and streamlined governance (Watts, 2023). Together, these safeguards are designed to not only mitigate risks but to transform cyber resilience into a national competitive advantage.

To achieve these goals, the Australian government has set a concise roadmap that spans three "horizons":

- **Horizon 1 (2023–2025):** Enhancing the foundations by concentrating on the uplift of baseline resilience, cyber hygiene and imperative reforms.
- **Horizon 2 (2026–2028):** Strengthening resilience by aligning with international frameworks, scaling national threat intelligence and fostering public-private collaboration.
- **Horizon 3 (2029–2030):** Global leadership — establishing Australia as a trusted digital partner and exporter of cyber expertise throughout the Asia-Pacific region (Austrade, 2023).

The Australian government and industry will work together to enhance the cyber shields and build our national cyber resilience.

Source: Department of Home Affairs

Regulatory and policy reforms to raise the cybersecurity baseline

Several regulatory and policy reforms underpin the 2023–2030 Cyber Security Strategy, forming the backbone of Horizon 1 (2023–2025). They include new legislative instruments, such as the Cyber Security Act 2024 and the Digital ID Act 2024, as well as expansions or updates to existing frameworks, including the SOCI Act, Privacy Act amendments, PSPF 2025 and APRA's CPS 230. These key measures collectively seek to uplift baseline resilience and embed robust governance across sectors. Following is a brief overview of the regulations.

Cyber Security Act 2024

On 29 November 2024, the Cyber Security Act 2024 received Royal Assent. This gave legislative effect to several measures in the national strategy, including mandatory smart device standards, a ransomware and extortion payment reporting regime (CISC, 2025), limited-use protections for information shared with government, and the creation of a Cyber Incident Review Board (Parliament of Australia, 2024).

Mandatory ransomware payment reporting

As part of the Cyber Security Act 2024, commencing in 2025, organisations with annual turnover equal to or greater than $3 million are required to report any ransomware or extortion payments within 72 hours to the Cyber and Infrastructure Security Centre (CISC), part of the Department of Home Affairs, using prescribed information fields. This obligation creates greater transparency and accountability for how businesses respond to cybercrime (CISC, 2025).

Organisations with annual turnover equal to or greater than $3 million are required to report any ransomware or extortion payments within 72 hours to the Cyber and Infrastructure Security Centre (CISC) using prescribed information fields.

Digital ID Act 2024

The Digital ID Act 2024 commenced on 1 December 2024, creating a legal framework for accreditation, governance and privacy protections in Australia's national Digital ID system. It enables government-recognised digital identities to be adopted more broadly by both public and private sector organisations (Digital ID Act, 2024).

Security of Critical Infrastructure (SOCI) Act Expansion

The SOCI Act, which originally applied to just four sectors (electricity, gas, water and ports), was expanded through the 2021 amendments to the SOCI Act, which increased coverage from four sectors to 11 critical infrastructure sectors — communications; financial services and markets; data storage or processing; defence industry; higher education and research; energy; food and grocery; healthcare and medical; transport; water and sewerage; and space technology. The sectors are further broken down into 22 defined asset classes, each potentially subject to varying obligations depending on its classification. Subsequent 2022 amendments (SLACIP Act) introduced further obligations such as critical infrastructure risk management programs (CIRMPs), Systems of National Significance, and enhanced government step-in powers (CISC, 2025).

The primary responsibilities under the expanded SOCI Act are as follows:

- Cyber and operational hazards need to be addressed through CIRMPs.
- Mandatory notification of cyber incidents within 12–72 hours.
- The government has the authority to "step in" and manage nationally significant incidents.

Amendments to Privacy Act 1988

In December 2024, Parliament passed amendments to the Privacy Act 1988. Key changes included introducing civil penalties for serious invasions of privacy (in force since 10 June 2025), criminal penalties for doxxing, enhanced transparency rules on automated decision-making (with some requirements effective from 10 December 2026), and expanded powers for the Office of the Australian Information Commissioner to initiate investigations, compel information, and coordinate enforcement with other regulators (Attorney-General's Department, 2024).

The maximum penalties for significant breaches were increased to the greater of $50 million, three times the value of any benefit obtained from the contravention, or 30% of the organisation's adjusted turnover during the breach period. These changes are reflected in the Attorney-General's privacy reform materials and in subsequent OAIC enforcement guidance. (Attorney-General's Department, 2024; OAIC, 2023).

Protective Security Policy Framework (PSPF 2025)

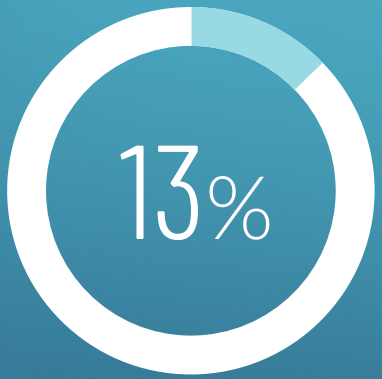
Released in July 2025, PSPF 2025 mandates adoption of Zero Trust principles across Commonwealth entities and replaces the Gateway Security Policy with a mandatory Gateway Security Standard. This standard requires modernised gateway architecture, integration of threat intelligence, and continuous monitoring. The PSPF continues to span six domains — governance, risk, information, technology, personnel and physical — but with stronger emphasis on critical digital services and supply chain assurance (Protective Security Policy Framework, 2025).

Australian Prudential Regulation Authority's (APRA) CPS 230 (Operational risk management)

On 1 July 2025, APRA's cross-industry prudential standard, CPS 230, took effect, reinforcing obligations for banks, insurers, and superannuation funds around operational risk management, business continuity, and service provider oversight (APRA, 2025), with linkage to CPS 234 Information Security standard.

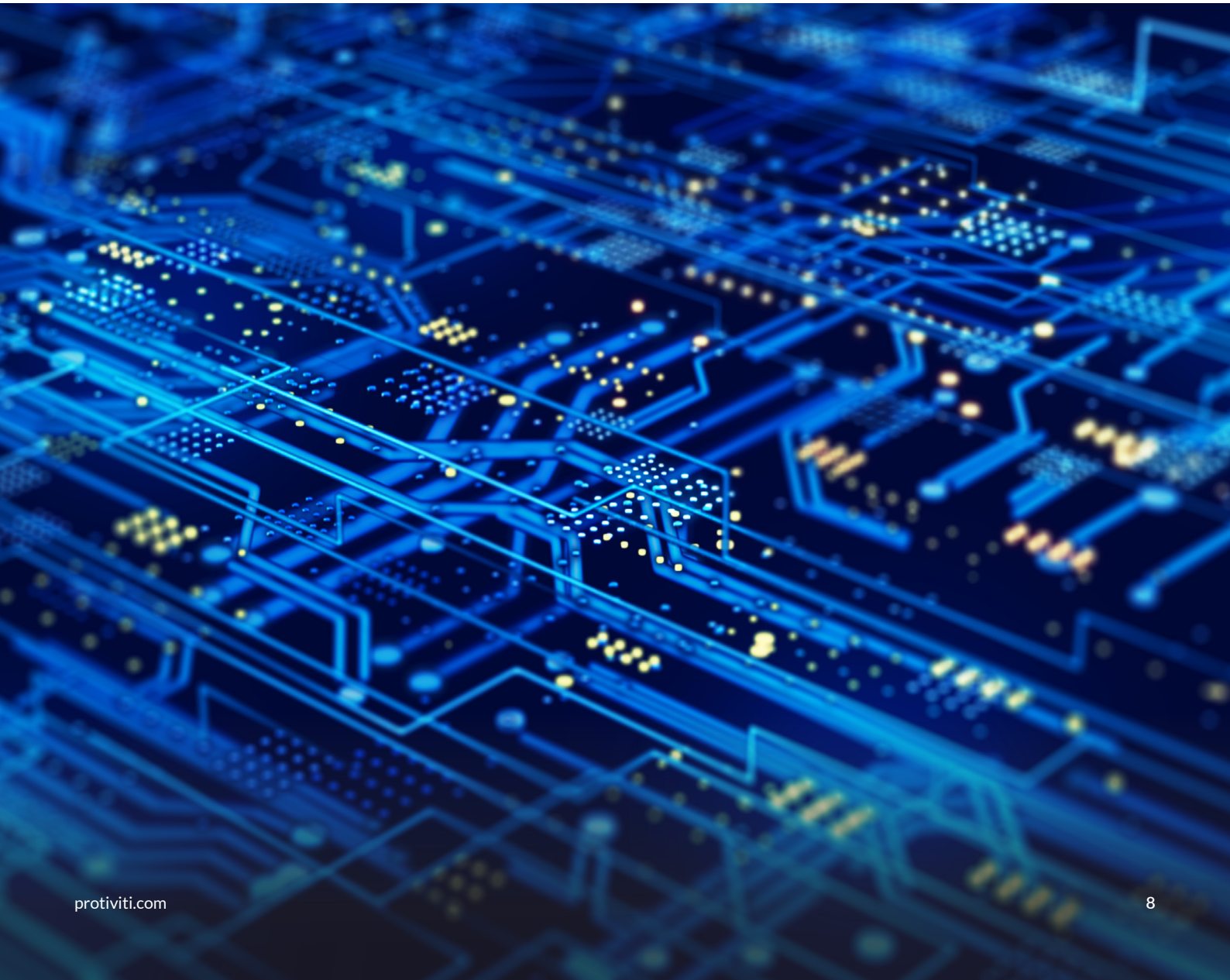
Financial services accounted for 13% of total cyber crime losses in 2022–23.

Source: Annual Cyber Threat Report, 2023



Industry impacts: How the reform is reshaping business

Cyber reforms now permeate all sectors of the Australian economy. Each industry faces unique obligations, timelines and challenges — while also being shaped by whole-of-economy reforms like the Cyber Security Act 2024, SOCI Act, Digital ID Act 2024, and Privacy Act 1988 amendments. Below is a brief overview for each sector with impacts, opportunities and challenges.



Financial Services Sector (Banking & Capital Markets)

Financial institutions are at the forefront of regulatory uplift, given their role in economic stability and attractiveness as high-value cybercrime targets.

Challenges:

- Multiple overlapping regulatory frameworks.
- Cloud concentration risk: Over 75% of major banks rely on fewer than three cloud providers (APRA, 2023).
- High exposure: Financial services accounted for 13% of total cyber crime losses in 2022–23 (ACSC, 2023).

Regulatory requirements:

- APRA CPS 230 (Operational Risk Management): Effective 1 July 2025.
- SOCI Act: Applies to financial market infrastructure; requires CIRMPs and incident notification within 12–72 hours.
- Privacy Act 1988 (as amended in 2024): New tort and a doxxing criminal offence from 10 June 2025; automated decision-making transparency obligations from 10 December 2026.
- Cyber Security Act 2024: Commenced on 29 November 2024, with ransomware/extortion payment reporting obligations effective from early 2025 and mandatory smart device security standards being phased in from mid-2025 (Parliament of Australia, 2024; CISC, 2025).

Expected impact:

Expanded investments in cloud resilience, improved operational risk governance and monitoring, and third-party oversight.

Opportunity:

Position Australia as a regional hub of cyber-resilient finance.

Government and Public Sector

Government agencies are central to national cyber resilience, holding critical citizen data and delivering essential services.

Challenges:

- Legacy IT barriers: Many systems not designed for Zero Trust.
- Workforce shortages: In the 2024 PSPF survey, 25% of agencies cited staff shortages as barriers to compliance (PSPF, 2025).

Regulatory requirements:

- PSPF 2025: From July 2025, adoption of Zero Trust principles and compliance with the Gateway Security Standard.
- Digital ID Act 2024: In force from 1 December 2024, governs accreditation and use of digital identity across agencies.
- Privacy Act 1988 (as amended in 2024): Office of the Australian Information Commissioner (OAIC) was granted expanded enforcement powers — including the ability to initiate investigations, compel information, issue infringement notices, and coordinate with other regulators (Attorney-General's Department, 2024).
- Cyber Security Act 2024: Mandatory ransomware/extortion payment reporting (commencing 2025) for agencies above the reporting threshold (Parliament of Australia, 2024; CISC, 2025).

Expected impact:

Elevated expectations for digital service resilience.

Opportunity:

Leadership in secure, trusted e-government services.

Energy and Utilities

Energy providers and utilities face systemic risk, as cyber incidents can trigger physical safety issues and national disruption to critical services.

Challenges:

- Operational technology (OT)/IT integration complexity; Industrial control systems (ICS) often insecure by design.
- Ransomware risk: The sector accounted for 15% of ransomware incidents in 2022–23 (ACSC, 2023).

Regulatory requirements:

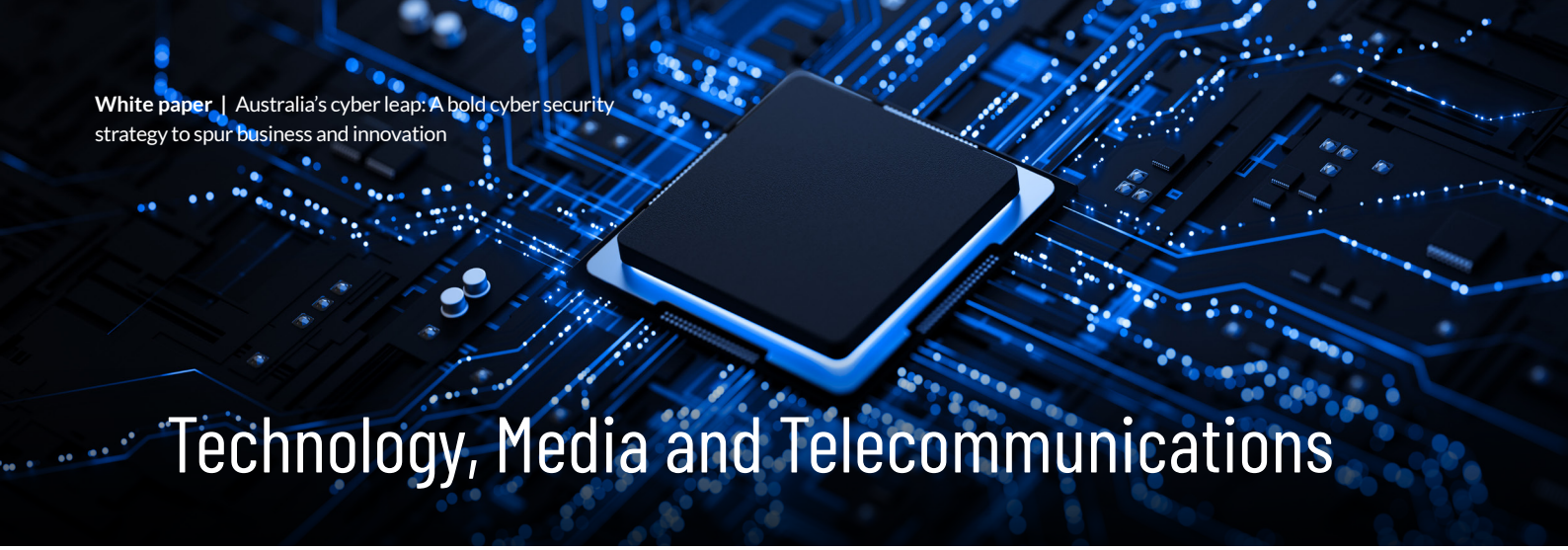
- Privacy Act 1988 (as amended in 2024): Strengthened requirements for protecting customer and employee data, introducing mandatory breach notifications, governance over automated systems, and higher penalties to align privacy compliance with critical infrastructure obligations.
- SOCI Act: CIRMP obligations phased from 2023; updated in 2025 (CISC, 2025).
- Cyber Security Act 2024: Mandatory ransomware/extortion payment reporting (commencing 2025) and Smart device standards relevant for IoT-enabled metering and grid technology (Parliament of Australia, 2024).

Expected impact:

Increased investment in OT security and sovereign threat intelligence.

Opportunity:

Environmental, social and governance (ESG)-aligned resilience strengthens trust with regulators and investors.



Technology, Media and Telecommunications

TMT companies operate Australia's digital backbone and are frequently targeted due to the value and volume of customer data.

Challenges:

- Telco breaches: OAIC reported that telecommunications accounted for the largest share of breached records in 2022–23 (OAIC, 2023).
- 5G/6G expansion multiplies attack surfaces.

Regulatory requirements:

- SOCI Act: Applies to telecommunications, data storage and broadcasting infrastructure.
- Cyber Security Act 2024: Mandatory ransomware reporting and smart device standards.
- Privacy Act 1988 (as amended in 2024): Higher penalties and new privacy rights (Attorney-General's Department, 2024).
- CPS 230 Information Security standard (as material provider to the financial services sector).

Expected impact:

Greater liability for network resilience.

Opportunity:

Secure-by-design infrastructure as a competitive differentiator.

Telcos accounted for the largest share of breached records in 2022-2023.

Source: Office of the Australian Information Commissioner, 2023

Healthcare and Life Sciences

Healthcare entities are high-value targets due to sensitive personal data and critical service delivery.

Challenges:

- The Medibank breach of 2022 exposed 9.7 million records; remediation costs: ~$250 million (Parliament of Australia, 2023).
- Healthcare remains the sector with the highest number of breach notifications, followed by the finance sector (ACSC, 2023).

Regulatory requirements:

- SOCI Act: Hospitals and pharmaceutical supply chains classified as critical assets.
- Privacy Act 1988 (as amended in 2024): Stronger protections for health data.
- Cyber Security Act 2024: Ransomware reporting obligations critical to healthcare providers.

Expected impact:

Increased compliance and monitoring costs.

Opportunity:

Trusted, secure digital health platforms to build patient confidence.

The cost for remediating the Medibank breach of 2022 was $250 million.

Source: Parliament of Australia, 2023

Education and Research

Universities and research institutions face dual risks: foreign interference and financial pressures.

Challenges:

- Espionage risk: Foreign actors are actively targeting Australian research IP (ASPI, 2025; Department of Home Affairs, 2023).
- Funding constraints: Smaller universities lack resources; North South Wales (NSW) Audit Office flagged deficits delaying cyber uplift. (NSW Audit Office, 2024).

Regulatory requirements:

- SOCI Act: CIRMPs and incident reporting within 12–72 hours.
- Digital ID Act 2024: Applies to student and researcher identity ecosystems.
- Privacy Act 1988 (as amended in 2024): Expanded obligations for student and research data.
- Cyber Security Act 2024: Mandatory ransomware/extortion payment reporting (commencing 2025), relevant given the sector's rising exposure to extortion campaigns (Parliament of Australia, 2024; CISC, 2025).

Expected impact:

Institutions with limited resources face growing risk exposure.

Opportunity:

Universities that invest in cyber resilience can attract global grants and partnerships.

Retail and Consumer Products and Services

Retailers manage vast amounts of personal and transactional data through loyalty and e-commerce platforms.

Challenges:

- OAIC reported 26% of breaches in 2023 involved consumer-facing sectors (OAIC, 2023).
- Rising compliance costs in low-margin environments.

Regulatory requirements:

- Privacy Act 1988 (as amended in 2024): New tort and higher penalties effective from 10 June 2025.
- Cyber Security Act 2024: Mandatory ransomware reporting obligations commenced in early 2025.

Expected impact:

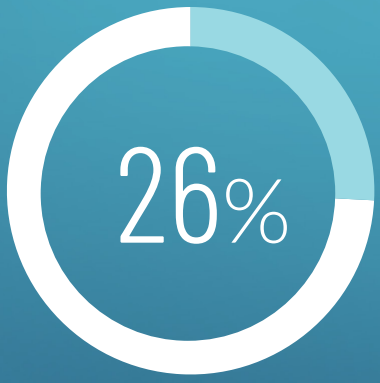
Greater reputational damages from breaches.

Opportunity:

Secure-by-design branding can be a differentiator in a competitive market.

26% of breaches in 2023 involved consumer-facing sectors.

Source: Office of the Australian Information Commissioner, 2023



Defence and Space

Defence and space are not only critical infrastructure sectors under the SOCI Act — they are also global growth industries for Australia, tightly linked to national security, trade, and international alliances.

Challenges:

- High-value IP theft: Foreign interference campaigns routinely target Australian defence contractors and space research organisations (ASPI, 2025).
- Geopolitical exposure: Strategic projects (e.g., AUKUS, joint space initiatives) increase the risk profile of Australian organisations.
- Rise of state-linked ransomware as a geopolitical weapon.

Regulatory requirements:

- SOCI Act: Expanded coverage to defence industry contractors and space assets; requires CIRMPs and 12–72 hour incident notification (CISC, 2025).
- Cyber Security Act 2024: Mandatory ransomware/extortion payment reporting commencing in 2025 (Parliament of Australia, 2024; CISC, 2025).
- Privacy Act 1988 (as amended in 2024): Applies to handling of personnel and contractor data.
- PSPF 2025: Heightened requirements for classified projects, Zero Trust adoption, and gateway protections.

Expected impact:

Heightened scrutiny of contractors and research partners for compliance.
Loss of contract opportunities if breaches occur.

Opportunity:

Strengthens Australia's role as a trusted partner in international defence and space supply chains.

Transport and Logistics

Challenges:

- Increased IT/OT convergence risk in logistics systems (ports, aviation, freight).
- Growing ransomware threats targeting global logistics chains.

Regulatory requirements:

- SOCI Act: Ports, aviation, and freight covered by CIRMP and incident reporting obligations (CISC, 2025).
- Privacy Act 1988 (as amended in 2024): Stricter requirements to secure passenger, freight, and tracking data, timely breach notifications and transparency in automated logistics systems to strengthen accountability across digital supply chains.
- Cyber Security Act 2024: Ransomware/extortion payment reporting obligations apply from 2025 (Parliament of Australia, 2024; CISC, 2025).

Expected impact:

Increased investment needed in supply chain visibility, monitoring, and resilience testing.

Opportunity:

Increased trust in Australian transport corridors as secure trade gateways.

Food and Grocery

Challenges:

- Globalised supply chains create vulnerabilities.
- Ransomware and cyberattacks on logistics/distribution networks can directly impact food availability.

Regulatory requirements:

- SOCI Act: CIRMP obligations apply to ensure continuity of supply (CISC, 2025).
- Privacy Act 1988 (as amended in 2024): Stricter obligations for protecting customer and supplier data, including mandatory breach notifications, higher penalties, and transparency over automated systems used in ordering and logistics.
- Cyber Security Act 2024: Ransomware/extortion payment notification obligations from 2025 (Parliament of Australia, 2024; CISC, 2025).

Expected impact:

Higher compliance costs to secure distribution networks. Cyber incidents could directly affect ESG and food security reporting obligations.

Opportunity:

Cyber maturity becomes a differentiator in supplier negotiations with major retailers.

Manufacturing

Challenges:

- Legacy OT/ICS systems highly vulnerable to cyberattacks.
- Ransomware campaigns increasingly target manufacturing to cause operational downtime.

Regulatory requirements:

- SOCI Act & PSPF 2025: Critical manufacturing assets face resilience obligations, including CIRMPs and mandatory incident reporting (CISC, 2025; PSPF, 2025).
- Privacy Act 1988 (as amended in 2024): Expanded obligations to protect employee, supplier, and production data, mandatory breach notifications and governance over automated and AI-driven systems used in smart factories and supply chain operations.
- Cyber Security Act 2024: Mandatory ransomware/extortion payment reporting from 2025 (Parliament of Australia, 2024; CISC, 2025).

Expected impact:

Significant uplift in cybersecurity controls needed across OT environments. Higher audit and compliance burden for manufacturers embedded in critical supply chains.

Opportunity:

Integration of cyber resilience accelerates innovation and market positioning.

Shared challenges on the road to 2030

In addition to the industry specifics highlighted above, businesses in all sectors face the following common challenges and constraints:

- **Framework complexity:** There are overlapping obligations under the SOCI, Privacy Act, CPS 234 and 230, ISO 27001, NIST CSF and other regulations, making it difficult for businesses to understand where their gaps are and where to allocate resources.
- **Skills shortage:** The Australian Computer Society projects a deficit of 30,000–50,000 cyber professionals by 2030 (ACS, 2023). This means greater competition for talent and higher expenses.
- **Insurance gaps:** Rising premiums and more frequent policy exclusions means businesses will find it more difficult to rely on insurance as a financial safety net after a cyberattack. The higher out-of-pocket costs and increased financial risk, if targeted by ransomware makes robust cybersecurity measures and risk management even more critical.
- **Resource constraints:** Small and medium-sized enterprises (SMEs), which account for 97% of Australian businesses, will no doubt face the most challenges meeting the increased demands. However, they should view the new mandates as an opportunity for innovation and market differentiation, enhancing resilience and fostering greater trust with stakeholders. Organisations are encouraged to embed cybersecurity into core business strategies and invest in training, technology, and partnerships that align with compliance requirements, ultimately transforming risks into strategic advantages.

The Australian Computer Society projects a deficit of 30,000–50,000 cyber professionals by 2030.

Source: Australian Computer Society, 2023

How organisations can respond

To align with the Cyber Security Strategy, businesses should take a staged approach that mirrors the horizons set by the Australian government:

Fortify the foundations (2023–2025)

- Perform gap assessments against the amended Privacy Act, SOCI, and ACSC's Essential Eight Maturity Model.
- Implement mandatory procedures for incident response and reporting as required by the relevant acts:
  - 12-72-hour reporting for critical infrastructure incidents (SOCI Act).
  - 72-hour ransomware/extortion payment reporting, all sectors (Cyber Security Act 2024).
  - Reporting of operational risk incidents (including cyber incidents) to regulator (APRA CPS 230 and CPS 234).
  - Government agency incident response standards (PSPF, 2025).
  - Mandatory breach notification to OAIC, all sectors (Privacy Act/NDB scheme).
- Conduct executive cyber governance and awareness training.

Scale and integrate (2026–2028)

- Integrate cybersecurity into enterprise and operational risk management frameworks.
- Improve third-party and supply chain oversight and governance mechanisms, including due diligence procedures, service provider risk assessments, contract updates and contingency and exit planning.
- Engage in threat intelligence exchange networks led by the Australian Cyber Security Centre (ACSC).

Lead and differentiate (2029–2030)

- Invest in quantum-safe solutions and sovereign cyber capabilities to ensure independence, security, and innovation with minimal reliance on foreign suppliers.
- Assume the status of globally recognised leaders in cyber-resilient business, trusted by international partners, investors and customers.
- Consider cyber resilience to be a performance indicator at the board level.

From compliance to competitive advantage

The cybersecurity measures that Australia has implemented constitute a generational shift. In addition to being a defensive measure, the Cyber Security Strategy for the years 2023–2030 is also a roadmap for the construction of the nation, with businesses playing a major role in that vision. By embracing the strategy, industries have the opportunity to unlock innovation, gain a competitive advantage, and increase trust with citizens, customers, investors and global partners. Robust cybersecurity foundations can vastly accelerate adoption of advanced technologies like AI, IoT and quantum; and alignment with international frameworks can open new doors to cross-border commerce and partnership.

For boards of directors, executives and industry leaders, the choice is clear: they can either view the reforms as a burden of compliance, or they can view them as a strategic enabler and seize the opportunity to lead. Those who take decisive action will be able to flourish in an environment where cyber resilience is synonymous with business resilience.

How Protiviti can help

Protiviti is a strategic partner in implementing Australia's cybersecurity reform. We help clients translate intricate regulations into actionable compliance steps and design comprehensive cyber strategies consistent with digital transformation and ESG goals. We strengthen governance through the implementation of risk supervision frameworks and board training and encourage innovation through the secure implementation of artificial intelligence, analytics and identification systems. Learn more at Cybersecurity Strategy Consulting | Protiviti Australia and Cyber Defence & Incident Response | Protiviti Australia.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the *Fortune* 100 Best Companies to Work For® list for the 11th consecutive year, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti is a wholly owned subsidiary of Robert Half Inc. (NYSE: RHI).

Contacts

Hirun Tantirigama
Managing Director
hirun.tantirigama@protiviti.com.au

Chandrakant Kamble
Associate Director
chandrakant.kamble@protiviti.com.au

References

ACS. (2023). Cyber skills shortage report. Australian Computer Society. https://www.acs.org.au/content/dam/acs/acs-publications/Australias_Digital_Pulse_2023_Digital.pdf

ACSC. (2023). Annual cyber threat report 2022–23. Australian Cyber Security Centre. https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

APRA. (2023, September 21). APRA highlights risks in banks' heavy reliance on a small number of cloud service providers. Australian Prudential Regulation Authority. https://www.apra.gov.au/apra-explains-importance-of-managing-operational-risk

APRA. (2025). Prudential Standard CPS 230 – Operational Risk Management. Australian Prudential Regulation Authority. https://handbook.apra.gov.au/standard/cps-230

Attorney-General's Department. (2024). Privacy Act reforms (2024 update). Australian Government. https://www.ag.gov.au/rights-and-protections/privacy

Austrade. (2023, November 22). Australia's strategy to become a global cyber leader by 2030. Australian Trade and Investment Commission. https://international.austrade.gov.au/en/news-and-analysis/news/Australias-strategy-to-become-global-cyber-leader-by-2030

Australian Strategic Policy Institute. (2025, June 30). Shifting the needle: Making Australia's research security ecosystem work smarter. https://www.aspi.org.au/report/shifting-the-needle-making-australias-research-security-ecosystem-work-smarter

CISC (Cyber and Infrastructure Security Centre). (2025). Cyber security legislative reforms (SOCI obligations, CIRMP and reporting). Australian Government, Department of Home Affairs. https://www.cisc.gov.au/legislation-regulation-and-compliance/cyber-security-legislative-reforms

Department of Home Affairs. (2023, November 22). 2023–2030 Australian Cyber Security Strategy. Australian Government. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

Digital ID Act. (2024). Digital ID Act 2024 (Cth). Federal Register of Legislation. https://www.legislation.gov.au/C2024A00025/latest/text

NSW Audit Office. (2024). Universities 2023: Financial audit results and observations – including cyber security risk management. https://www.audit.nsw.gov.au/our-work/reports/universities-2023

OAIC. (2023). Notifiable Data Breaches Report: January to June 2023. Office of the Australian Information Commissioner. https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2023

Parliament of Australia. (2023). Medibank Private data breach inquiry report. House of Representatives Standing Committee on Health, Aged Care and Sport. https://www.oaic.gov.au/__data/assets/pdf_file/0025/221974/Australian-Information-Commissioner-v-Medibank-Private-Limited-concise-statement.pdf

Parliament of Australia. (2024). Cyber Security Act 2024 (Cth) (No. 98, 2024). Federal Register of Legislation. https://www.legislation.gov.au/Series/C2024A00098

Protective Security Policy Framework. (2025, July 24). PSPF Annual Release 2025 (incl. Gateway Security Standard and survey highlights). Australian Government. https://www.protectivesecurity.gov.au/publications-library/pspf-annual-release-2025

Protiviti. (n.d.). 2023 State of Play – Australian Privacy Reform. https://www.protiviti.com/au-en/whitepaper/2023-state-play-australian-privacy-reform

Protiviti. (n.d.). Australia's Privacy Act is fundamentally changing: What this means for your organisation. https://www.protiviti.com/au-en/blogs/australia-privacy-act-is-changing-what-this-means-for-your-organisation

Watts, T. (2023, November 22). 2023–2030 Cyber Security Strategy: A resilient region and global leadership. Department of Foreign Affairs and Trade. https://ministers.dfat.gov.au/minister/tim-watts/media-release/2023-2030-cyber-security-strategy-resilient-region-and-global-leadership

11,000+	90+	25+	$2 BN
Protiviti Professionals*	office locations worldwide	countries	in revenue*

THE AMERICAS

UNITED STATES
Alexandria, VA
Atlanta, GA
Austin, TX
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Columbus, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Indianapolis, IN
Irvine, CA
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte*
Rio de Janeiro
São Paulo

CANADA
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

BULGARIA
Sofia

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA*
Durban
Johannesburg

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Chennai
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

© 2025 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. 1125-AU-EN

protiviti®