protiviti®
Global Business Consulting

Australian Federal Budget 2026-27: Cyber investment rises – expectations rise faster

14 May
2026

The 2026–27 Federal Budget reinforces a clear and accelerating shift: Cyber security is no longer a technical discipline or standalone investment category. It is a core component of national resilience, economic stability and service delivery. Headline commitments include $654.3 million over four years to secure the Australian Government Digital ID System, a $160.4 million Cyber Security Uplift for Services Australia, and a further $89.3 million to sustain and enhance Commonwealth cyber security initiatives.

While continued funding signals commitment to strengthening Australia's cyber capability, it also raises expectations on organisations, particularly government agencies and regulated sectors — to demonstrate that cyber risks are actively governed, effectively controlled and independently assured.

For executive teams, the implications are immediate. The challenge is no longer whether cyber investments are being made, but whether they are:

- Delivering measurable risk reduction;
- Defensible under regulatory and public scrutiny; and
- Integrated into enterprise governance, risk and assurance structures

This paper outlines the key cyber themes emerging from the Budget and what they mean for senior executives, boards and audit committees.

1) Cyber security is now framed as national resilience, not an IT function.

What the Budget signals

The Federal Budget continues sustained investment in national cyber resilience, including a $160.4 million Cyber Security Uplift for Services Australia and $654.3 million over four years to maintain the security of the Australian Government Digital ID System.[1]

Cyber risk is increasingly positioned as a threat to economic stability and service delivery — not merely a technical vulnerability. Treasurer Jim Chalmers' framing of the Budget around "resilience and reform" — against a backdrop of geopolitical volatility and what he described as the fifth economic shock in under 20 years, situates cyber resilience squarely within the national economic security agenda.[2]

Protiviti perspective

Cyber security has firmly moved beyond the IT function. It is now a core enterprise risk that boards and executives are expected to actively govern and oversee. Organisations should consider the following questions:

- Do boards have clear visibility of cyber risk exposure and tolerance?
- Are accountabilities for cyber decision-making clearly defined across the executive suite?
- Is cyber risk embedded within enterprise risk frameworks — or operating in isolation?

2) Increased cyber funding raises expectations for demonstrable assurance.

What the Budget signals

Government investment in cyber capability is accompanied by rising expectations that agencies and organisations can **demonstrate cyber resilience**, not simply assert compliance.[1] The Budget commits $89.3 million over four years to sustain and enhance cyber security initiatives across the Commonwealth, alongside the $160.4 million Services Australia uplift, recurring investments that signal ongoing scrutiny rather than a one-off injection.[3]

Protiviti perspective

Increased funding does not reduce scrutiny, it intensifies it. Stakeholders, regulators and audit bodies will expect evidence that cyber controls are effective, operating as intended and delivering outcomes. Organisations should consider the following questions:

- Can leadership rely on reported cyber risk metrics?

Are controls independently validated or self-assessed?

- Is cyber maturity being measured meaningfully, beyond checklist compliance?

3) Mandatory cyber reporting is now law, not an emerging expectation.

What the Budget signals

The **Cyber Security Act 2024** introduced mandatory ransomware payment reporting, which commenced on 30 May 2025. Entities with annual turnover of $3 million or more, and responsible entities for critical infrastructure assets to which Part 2B of the SOCI Act applies, must report any ransomware or cyber extortion payment — whether made by the entity or on its behalf — to the Department of Home Affairs and the Australian Signals Directorate within 72 hours of the payment being made (or of becoming aware that a payment has been made). The Act also established the Cyber Incident Review Board.

The 2024 SOCI Act amendments clarified that risk management obligations extend to data storage systems holding business-critical data. Continued Budget investment in regulatory capability reinforces that these obligations will be actively enforced.[4]

Protiviti perspective

The direction of travel is clear: Organisations will need to explain not just what occurred in a cyber incident, but whether their controls were reasonable, proportionate and defensible. Organisations should consider the following questions:

- Are incident response frameworks structured for regulatory scrutiny?
- Is there clear governance over cyber incident decision-making?
- Can the organisation evidence the effectiveness of its control environment post-incident?

4) Cyber risk is increasingly intertwined with fraud and scams.

What the Budget signals

Ongoing funding for scam prevention, fraud detection and cross-agency coordination reinforces the convergence of cyber, fraud and integrity risks.[2,3]

Protiviti perspective

Cyber incidents are no longer discrete security events, they are often entry points to fraud, financial loss and reputational damage. Organisations should consider the following questions:

- Are cyber and fraud risk functions integrated or siloed?
- Are cyber controls aligned to fraud prevention outcomes?

Is there visibility across the full lifecycle, from breach to financial impact?

5) Digital identity and cyber trust are becoming core public infrastructure.

What the Budget signals

The Budget commits $643.6 million over four years to maintain the security of the Australian Government Digital ID System, spanning the ATO ($357.4m), Services Australia ($135.2m), the ACCC ($98.0m), the Department of Finance ($30.8m) and the OAIC ($22.2m). This aligns with the broader headline investment in Digital ID security and reinforces the system's role as critical public infrastructure, supported by statutory privacy safeguards under the Digital ID Act 2024.[5]

Protiviti perspective

Identity is emerging as the cornerstone of cyber resilience and a focal point for regulatory, privacy and trust expectations. Organisations should consider the following questions:

- Is identity governance clearly owned and managed at an executive level?
- Are privacy-by-design principles embedded into digital initiatives?
- Can identity and access controls be independently assured?

6) Cyber spending is tightening. Scrutiny on value for money is rising.

What the Budget signals

Cyber and technology investments are increasingly targeted and disciplined, with greater emphasis on prioritisation and measurable outcomes.[3]

Protiviti perspective

In a constrained fiscal environment, the key question is not how much is being spent on cyber — but whether that spend is reducing enterprise risk in a demonstrable way. Organisations should consider the following questions:

- Are cyber investments aligned to enterprise risk priorities?
- Can organisations demonstrate return on cyber investment?

Is the cyber portfolio optimised or expanding without clear outcomes?

7) AI is now part of the cyber control environment.

What the Budget signals

Government investment in AI capability, scam disruption and Digital ID assumes a threat environment in which AI strengthens defenders and accelerates attackers in equal measure. This includes "agentic AI" — AI systems that can plan, make decisions and take actions autonomously across multiple tools and environments with limited human intervention. Guidance from ASD's ACSC on the cyber security implications of these technologies reframes AI as part of the control environment, not an adjacent issue. [6]

Protiviti perspective

AI is rapidly compressing the gap between cyber risk and fraud risk — deepfake-enabled social engineering, AI-generated scams and autonomous agent misuse are converging on the same control failures. Boards should expect to be asked how AI is governed within the cyber control environment, not only how cyber is governed within AI. Organisations should consider the following questions:

- Is AI use across the enterprise inventoried, classified and risk-rated?

Do existing cyber controls address emerging AI risks, including:

  - Agentic AI misuse (autonomous systems making unintended or harmful decisions),
  - Prompt injection (manipulating AI inputs to produce unsafe or misleading outputs), and
  - Model supply chain risks (vulnerabilities introduced via third-party AI models or training data)?

Is the workforce equipped to detect AI-enabled threats such as:

  - Phishing attacks enhanced by AI-generated content,
  - Deepfakes (realistic but fake audio, video or images used for deception), and
  - Synthetic identity fraud (fabricated identities created using real and fake data to bypass controls)?

What executive teams should reassess in the next 90 days

The Budget signals a shift from **investment to accountability**.

Executive teams should prioritise:

- **Cyber governance**
    - Clear ownership and board visibility of cyber risk
- **Assurance readiness**
    - Independent validation of control effectiveness
- **Incident defensibility**
    - Governance, evidence and decision frameworks for scrutiny
- **Cyber-fraud integration**
    - Alignment between cyber events and financial risk
- **Identity and trust**
    - Strengthening identity as a core control environment
- **Investment discipline**
    - Ensuring cyber spend delivers measurable enterprise outcomes
- **AI risk posture**
    - Embedding AI exposure and agentic AI risks into the cyber control environment

How Protiviti can help

Protiviti supports organisations in responding to rising cyber accountability expectations by strengthening governance, assurance, defensibility and value realisation across the enterprise. We can help in the following areas:

Cyber governance and risk clarity

Board and executive cyber risk clarity frameworks, governance and accountability model design, and integration of cyber risk into enterprise risk management and assurance.

Independent assurance and control effectiveness

Independent cyber assurance and readiness reviews, control effectiveness assessments aligned to enterprise risk, and maturity-based cyber assessments beyond baseline frameworks.

Incident governance and defensibility

Incident response governance and decision-rights frameworks, evidence-based control defensibility assessments, and executive readiness for post-incident review and regulatory inquiry.

Cyber-fraud integration

Integrated cyber-fraud risk frameworks, alignment of cyber controls to fraud detection and prevention, and improved coordination across risk, finance, cyber and internal audit.

Identity, privacy and trust

Identity governance and accountability frameworks, privacy-by-design advisory and assurance, and independent Identity and Access Management (IAM) effectiveness reviews.

Cyber investment and value realisation

Cyber investment prioritisation frameworks, benefits realisation and ROI modelling, and portfolio optimisation aligned to measurable risk reduction outcomes.

AI risk and control integration

AI risk and control posture assessments aligned to ACSC and ASD guidance, integration of AI governance with cyber, privacy and fraud frameworks, and board-level briefings on emerging AI threats and defensible response.

End notes

1. Commonwealth of Australia, *Budget 2026–27, Budget Paper No. 2: Budget Measures*, 12 May 2026 (budget.gov.au).
2. The Hon. Dr Jim Chalmers MP, *Budget Speech 2026–27*, House of Representatives, 12 May 2026.
3. King & Wood Mallesons, *Federal Budget 2026–27: Digital economy, cyber and Digital ID measures*, May 2026.
4. *Cyber Security Act 2024* (Cth); *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* (Cth).

5. *Digital ID Act 2024* (Cth); Department of Finance, Australian Government ID System program documentation
6. Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) et al., *Careful adoption of agentic AI services*, May 2026. Joint Five Eyes guidance led by ASD's ACSC in collaboration with CISA (US), NSA (US), the UK National Cyber Security Centre, the Canadian Centre for Cyber Security, and New Zealand's NCSC.

Contacts

Rita Gatt
Managing Director, Technology Consulting

Rich Turley
Managing Director, Internal Audit

Hirun Tantirigama
Managing Director, Technology Consulting

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps clients transform and protect their businesses and respond to planned and unexpected events. Through a network of more than 90 offices in over 25 countries, Protiviti and its independent and locally owned member firms deliver deep expertise and tailored capabilities across technology, artificial intelligence, data, operations, finance, legal, compliance, HR, marketing, digital, risk, and internal audit—enabling organisations to accelerate innovation, navigate risks and safeguard what matters most.

Named to the **Fortune 100 Best Companies to Work For®** list since 2015, Protiviti Inc. 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 Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

protiviti®