PUBLIC SECTOR NETWORK

Certified B Corporation

STATE OF THE SECTOR

CYBER SECURITY & RISK MANAGEMENT 2024-2025

EMERGING TRENDS, ANALYTICS AND FORECASTING

Editor's Introduction

Cybersecurity has evolved from a technical discipline to a strategic imperative—central not only to digital operations, but to public trust and institutional resilience. As governments across Australasia accelerate transformation efforts, the question is no longer whether security is a priority, but how effectively it is being embedded into organisational decision-making, investment, and culture.

This report presents an up-to-date snapshot of the public sector's cybersecurity posture, drawn from national polling conducted across jurisdictions. It explores how agencies are defining maturity, allocating resources, identifying threats, and assessing their own readiness. What emerges is not simply a checklist of security measures, but a layered portrait of how capability, culture, and confidence vary across the region.

Some findings confirm long-observed patterns: phishing remains a top concern, cultural change remains a work in progress, and most organisations are still striving to shift from compliance to resilience. Other insights challenge assumptions—particularly around the uneven uptake of advanced threat modelling, the under-recognition of human error, and the low prioritisation of impact-heavy threats like ransomware.

Above all, this report aims to move beyond surface-level benchmarks. It highlights not just what public sector agencies are doing to improve their cybersecurity, but how their approaches differ—and what those differences signal for strategic progress across the region.

We trust these insights will inform more targeted investment, more honest internal assessments, and ultimately, more secure digital futures.

Patrick Joy
Head of Research & Advisory
Public Sector Network

Research, Analytics and Methodology

Public Sector Network collects data from public sector professionals utilising real-time polling via an extensive, international events portfolio. This ensures a controlled environment that both anonymises respondent information while also ensuring the data comes from those working in the public sector. Event attendance is tracked and qualified through a registration list, which monitors participant job functions and respective portfolio agencies. Consequently, findings are rooted in direct participant input, providing a transparent and authentic representation of stakeholder views.

The aim of polling PSN attendees is to provide public sector insights that are both timely and highly relevant to the issues discussed. This polling data was collected across a series of events held in ANZ in 2024 to hundreds of event attendees.

The same five questions were posed at every event, and are listed as follows:

- **How would you rate your organisation's cybersecurity maturity level?**
- **What is your biggest barrier to reaching improved cyber security**
- **What are your main priorities for the next 12-18 months**
- **What are the biggest threats you are working to protect against?**
- **How do you assess the effectiveness of your organisation's cybersecurity measures?**

Finding 1: The Maturity Curve

National Average

The data reveals a pronounced clustering around intermediate cybersecurity maturity (43%). While this suggests a broadly embedded baseline of cybersecurity governance, it also indicates a potential stagnation point where many jurisdictions appear to have plateaued.

The low adoption of advanced cybersecurity capabilities—only 16% nationally—raises critical questions about the sector's capacity to shift from compliance-driven approaches to adaptive, intelligence-led cyber defence. This shortfall suggests a systemic hesitation or resource constraint in pursuing continuous improvement and threat hunting initiatives, both of which are becoming essential in a rapidly evolving risk environment.

Collectively, the data suggests that public sector cybersecurity strategies are still disproportionately focused on establishing control, rather than on enhancing resilience. Bridging this gap will require not only investment, but cultural and strategic shifts in how cyber risk is prioritised.

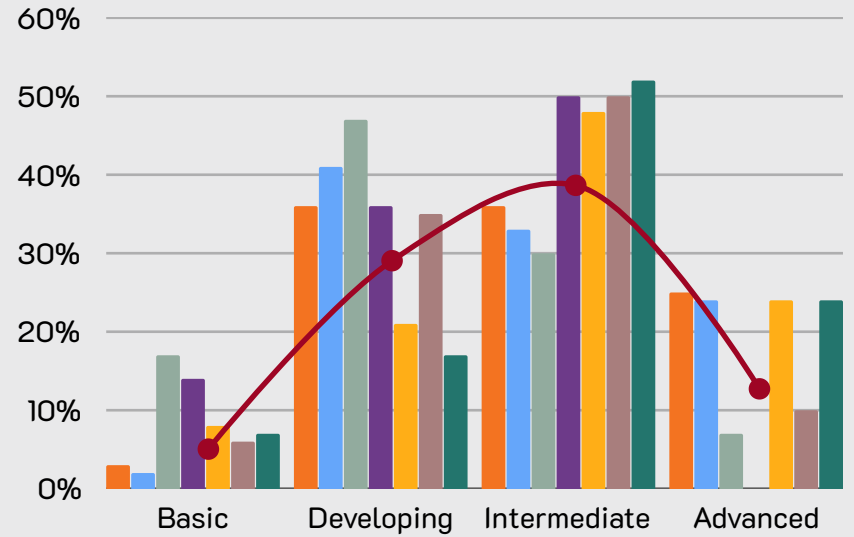
Outliers

- New Zealand purports the most mature cybersecurity landscape, with over half of respondents citing intermediate levels and a further 24% advanced.

- Western Australia reflects a duality. While 50% report intermediate maturity, none report advanced capabilities.

- South Australia skews significantly toward the developing stage (47%), the highest in the region, along with the highest basic response rate (17%). This indicates systemic constraints, more critical and comprehensive self-evaluation, or a potentially slower maturity trajectory.

How would you rate your organisation's cybersecurity maturity level?



- **Basic:** Limited cybersecurity measures and reactive approaches
- **Developing:** Some cybersecurity policies and procedures in place, but room for improvement
- **Intermediate:** Defined cybersecurity program with regular assessments and controls
- **Advanced:** Mature cybersecurity program with proactive threat hunting and continuous improvement initiatives

Total Sample: 407 Government Cyber Executives, Directors, and Specialists

Finding 2:

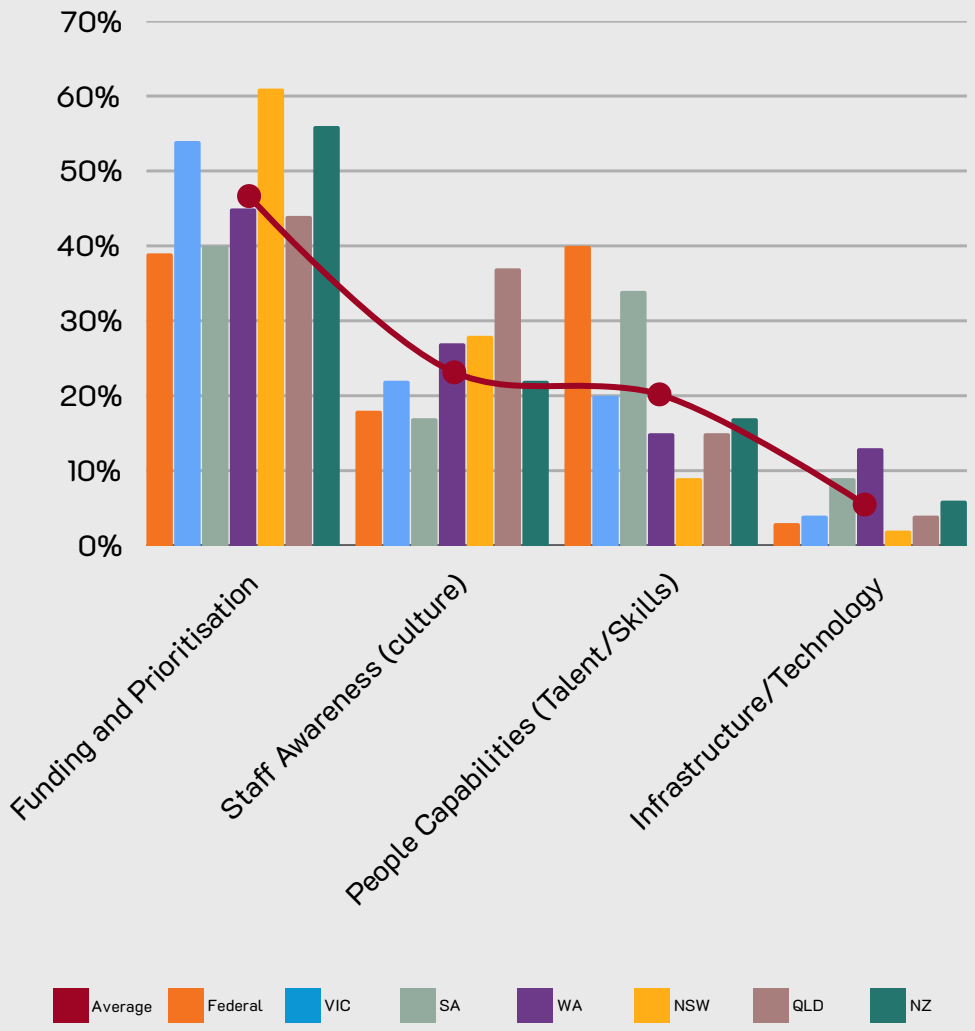
National Average
Funding and prioritisation emerge as the most significant constraint to cybersecurity progress, cited by nearly half (48%) of respondents. This underscores a fundamental misalignment between cyber risk awareness and the budgetary or strategic commitments needed to position cybersecurity as enabling operational pillar rather than a cost centre.

The human challenge persist across staff awareness and culture (24%) and people capabilities (21%) signalling awareness that technical defences are only as effective as the culture, skills, and talent required to operationalise sophisticated cybersecurity strategies.

Together with the relatively lower score for infrastructure and technology (6%) , these results paint a picture of a public sector that is not resource-starved in a technical sense, but is structurally under-equipped.

Outliers

- NSW stands out with 61% naming funding and prioritisation as their top barrier—highest of any region, despite NSW's relatively strong maturity.
- Federal Government and SA differ from the national trend, with notably high concern for people capabilities—40% and 34% respectively.
- WA is unique in elevating infrastructure and technology as a barrier (13%), nearly double the national average. This may reflect legacy challenges or uneven technology modernisation state-wide.



Total Sample: 442 Government Cyber Executives, Directors, and Specialists

Finding 3:

National Average

The primary cybersecurity objective for ANZ public sector over the next 12 to 18 months is creating a culture of cybersecurity (43%). This reflects a growing recognition that without organisational buy-in—across leadership, operations, and end-users—technical controls alone will not be sufficient. Culture has become the new cybersecurity control surface.

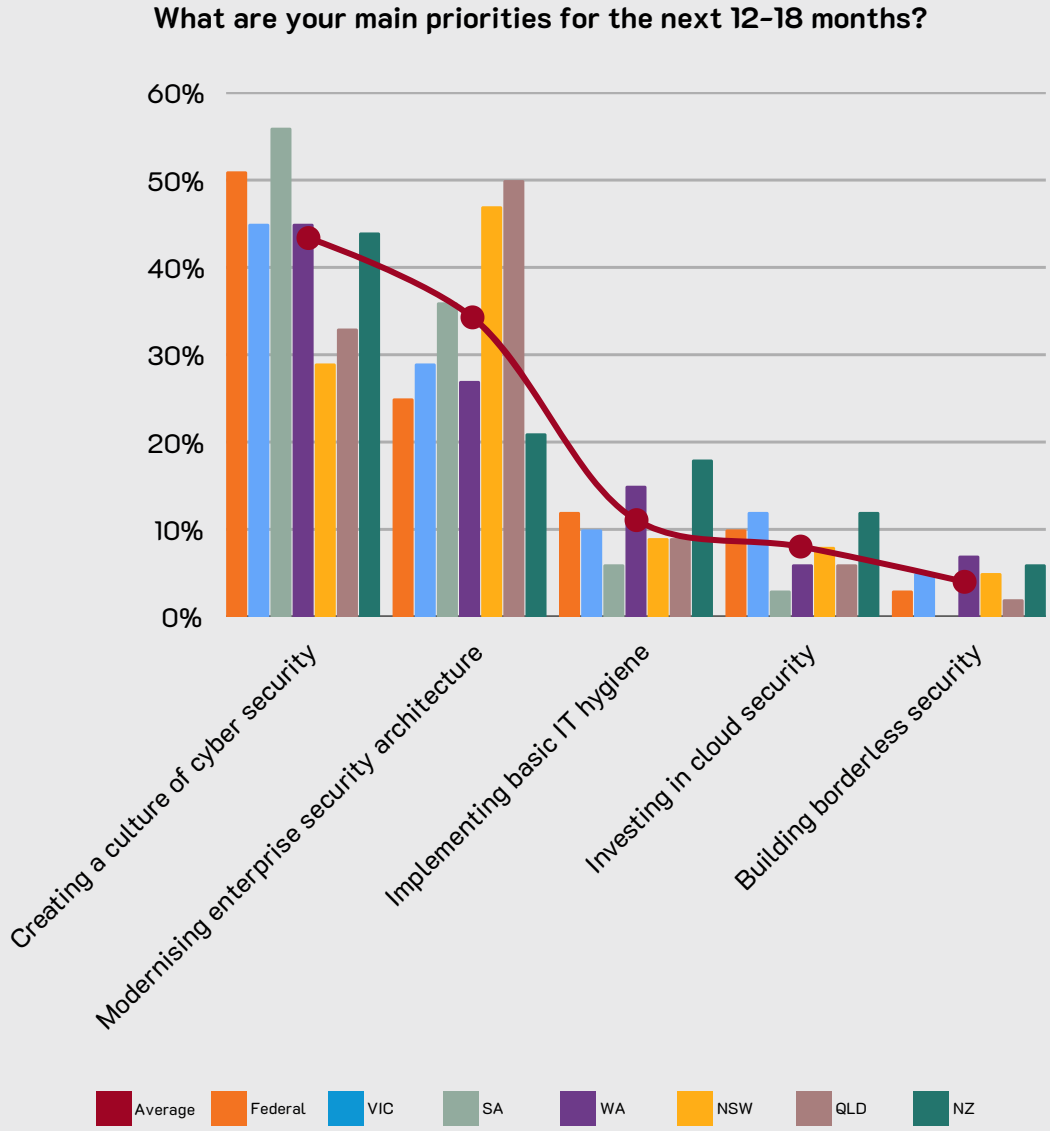
Close behind, modernising enterprise security architecture (34%) signals an ongoing shift from perimeter-based defence to integrated, identity-centric and zero-trust models in response to evolving threat complexity.

Only 11% cite implementing basic IT hygiene as a priority. While low on the list, this figure could be interpreted positively, in that many agencies may have already addressed foundational hygiene controls; or concerningly, in that some may be prematurely focusing on cultural or architectural goals before fully resolving baseline weakness.

Cloud security (8%) and borderless security (4%) register as the lowest priorities nationally, suggesting that many public sector agencies are still struggling to reconcile modern infrastructure and security trends with their planning cycles.

Outliers

- SA leads all jurisdictions in prioritising cyber culture (56%), perhaps in response to earlier findings indicating maturity and resource constraints.
- QLD and NSW show the strongest lean toward architecture modernisation (50% and 47%), pointing to technical overhaul mindset despite differing maturity.
- Central NZ is notably more invested in basic IT hygiene (18%) and cloud security (12%) than AU counterparts.



Total Sample: 453 Government Cyber Executives, Directors, and Specialists

Finding 4:

National Average

Phishing and social engineering attacks are the most frequently cited threats by public sector respondents (44%)—a view validated by the OAIC's breach data, where phishing accounts for the largest share (31%) of all cyber incidents.

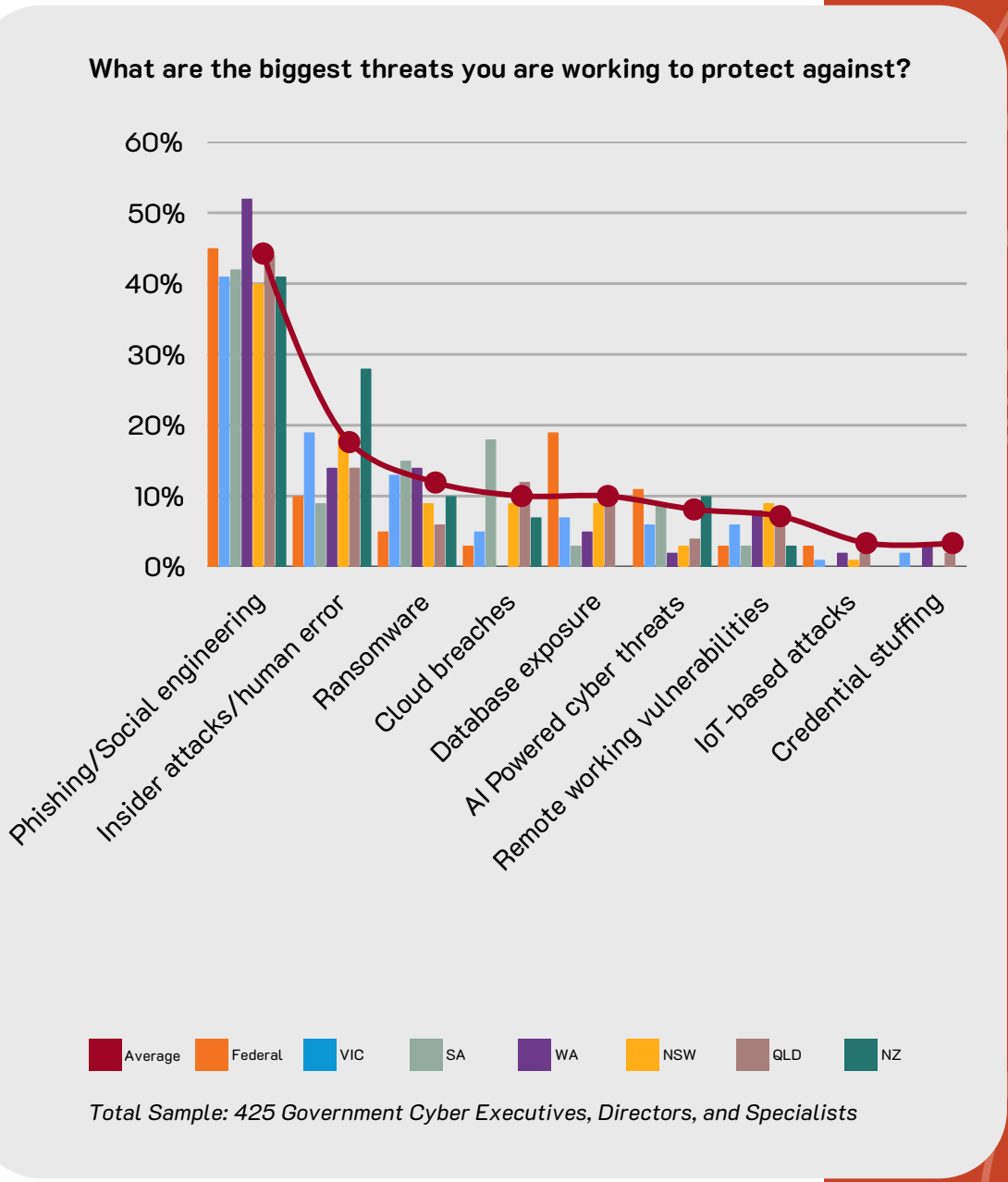
However, insider threats and human error are comparatively under-prioritised (16%), despite accounting for nearly one-third of all reported breaches—highlighting a critical disconnect between perceived and actual risk.

Ransomware, similarly, was selected by only 10% of respondents, yet represented 24% of actual cyber incidents—the second most common incident alongside compromised credentials, also 24%. Yet, ransomware events also carried outsized consequences, affecting an average of 295,555 individuals per breach, compared to just 709 for phishing.

To strengthen cyber resilience, agencies must plan not only for what's most likely—but for what can do the most harm.

Outliers

- WA leads all jurisdictions in concern about phishing (52%), suggesting either a higher volume of attempted attacks or more frequent user exposure.
- SA registers the highest concern for cloud breaches (18%), possibly linked to recency bias in migration efforts.
- Federal AU is the only jurisdiction to flag database exposure as a leading threat (19%), which may reflect the volume or sensitivity of data held by federal agencies.
- NZ diverges most significantly by ranking insider threats/ human error (28%), more than any Australian jurisdiction.



Finding 5: Talent and collaboration will help government meet expectations

National Average

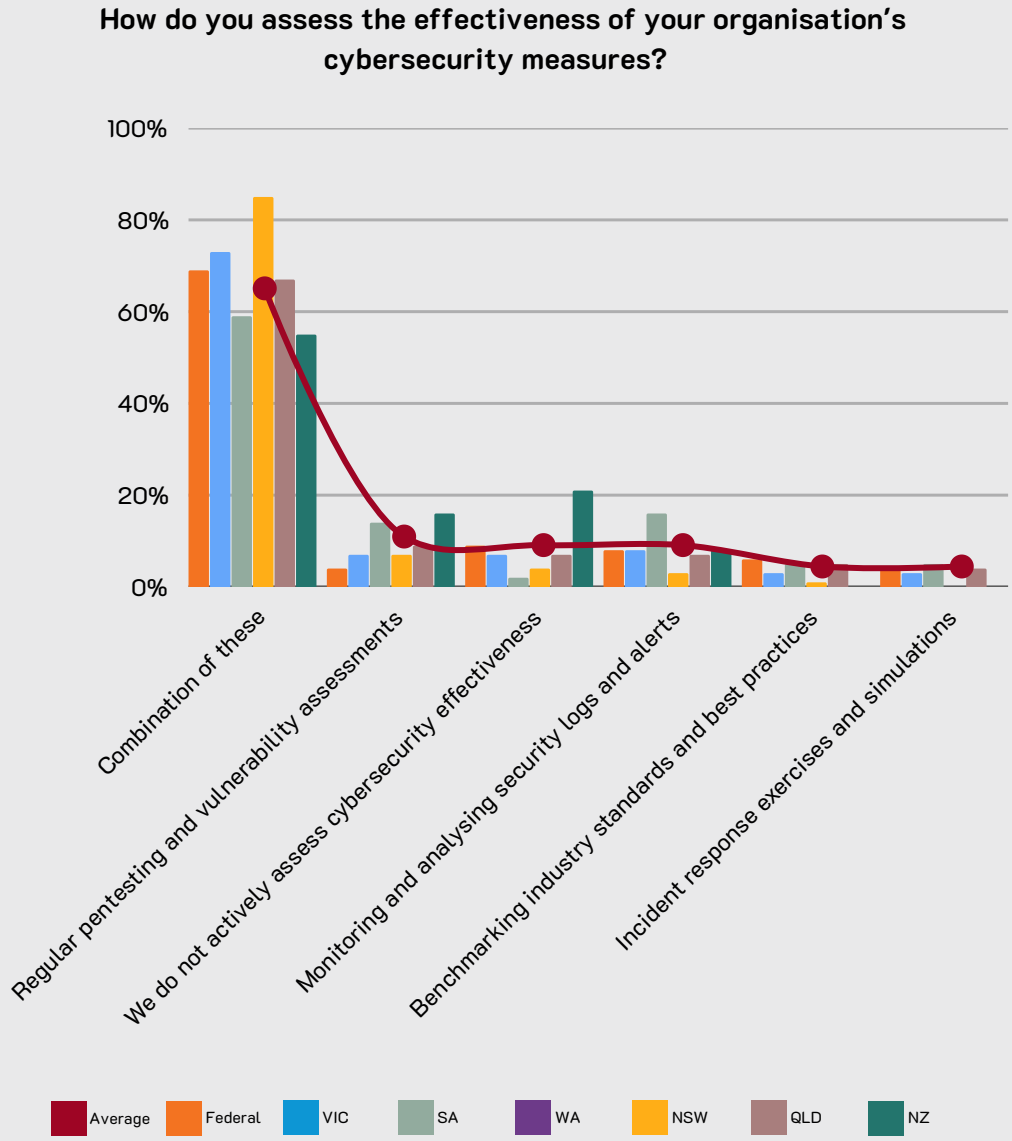
While the majority of respondents (68%) selected a combination of methods to assess cybersecurity effectiveness—an expected result—the deeper insight lies in how jurisdictions prioritise specific elements within that broader approach. The data reveals that even among those claiming a holistic posture, there are clear differences in what constitutes "effective".

Penetration testing and vulnerability assessments (10%) and log monitoring and analysis (8%) rank as the most commonly highlighted individual methods. This suggests that technical validation and real-time operational oversight are gaining traction as key indicators of cyber performance.

Alarmingly, 8% of organisations report that they do not actively assess their cybersecurity effectiveness. This signals a persistent maturity gap, particularly in jurisdictions where digital risk management remains underdeveloped or inconsistent.

Outliers

- NSW shows the most balanced maturity, with 85% of respondents using a combination of methods.
- NZ reflects the most fragmented maturity profile. 21% report no active assessment—the highest across all regions. Yet, NZ also leads in penetration testing (16%), suggesting a more audit-heavy approach.
- VIC (73%) and the ACT (69%) lead in adopting integrated assessment strategies, supported by moderate use of technical and monitoring tools. These jurisdictions appear to be more evenly distributing their assessment priorities across tactical and strategic domains.



Total Sample: 414 Government Cyber Executives, Directors, and Specialists

About PSN

Connecting Government Organisations Across the Globe

Our mission is to give public sector professionals a single place to come together, share ideas, and get free, unlimited access to the latest information about critical topics that are transforming the government landscape.

Our government-only network helps members to find relevant international content and case studies that are critical to your work and can help you save time and money. For those that are looking to network at a deeper level, we hold insightful events, ranging from conferences and exhibitions to intimate training courses and forums across major cities around the world.