Closing the Cyber Workforce Planning Gap for AI in Australia

Overview

This briefing note outlines how Australian leaders can strengthen workforce planning for AI and cyber-related risk based on comparisons of Australia's current posture with emerging approaches in Singapore, Saudi Arabia, and Canada. The central challenge for Australia is not a lack of activity, but a lack of integration between labour-market data, strategic planning, education pathways, and executive accountability.

Purpose

This note should help boards, senior public servants, and executive teams assess whether their current workforce planning is adequate for AI-driven changes in cyber risk, governance, and organisational ambition. It is supported by a practical checklist that can be used to stress-test planning assumptions against international practice.

Strategic context

Australia has taken meaningful steps, including the APS Data, Digital and Cyber Workforce Plan 2025–30 launched in March 2025. But implementation gaps are significant: more than half of APS agencies report critical cyber skills shortages, and the APS needs to roughly double its digital workforce by 2030. These plans have not yet consistently translated AI-related disruptions into capability planning for cyber, data, policy, and governance roles.

Singapore's SkillsFuture program offers a more integrated model, with strong alignment between government, education, labour-market intelligence, and industry needs. It explicitly links AI literacy and cyber resilience training to skills demand data, enabling faster adaptation to changing capability requirements than Australia's current settings allow.

Saudi Arabia has linked digital capability to national transformation through Vision 2030 and its dedicated agency, Saudi Data and Artificial Intelligence Authority (SDAIA). Sixty-six of ninety-six Vision 2030 goals relate to data and AI, with AI investment projected to reach USD 1.9 billion by 2027. This creates an explicit and measurable connection between national ambition and workforce development that Australia's decentralised settings do not currently replicate.

Canada's sector-based workforce planning offers a useful conceptual model linking demand forecasting, skills analysis, and training pathways. In practice, AI workforce training in Canada remains uneven and fragmented across sectors and regions. The lesson is the planning framework itself — specifically, how workforce demand can be connected to defined capability pipelines — rather than the consistency of its execution.

What this means for Australia

The main lesson for Australia is that workforce planning for AI-era cyber risk should be treated as a strategic governance issue, not only as an HR or operational matter. Organisations that rely only on historic staffing patterns or generic "digital skills" language are likely to underestimate the speed at which AI changes job design, decision-rights, and risk exposure.

Australian organisations should move from static planning to scenario-based planning over a three- to five-year horizon. That means testing what the workforce would need under conditions such as accelerated AI adoption, AI-enabled cyber threat escalation, stronger AI regulation, or tighter competition for specialist talent.

Priority questions for leaders

Boards and executive teams should ask whether they have identified the hybrid roles that now matter most, including roles that combine cyber, AI governance, data analysis, policy interpretation, and executive decision support. They should also ask whether there is a clear owner for workforce planning related to AI and cyber risk, and whether that planning is reviewed at senior decision-making level.

A further question is whether workforce plans are connected to actual capability pipelines. International practice shows the value of linking workforce demand to education, training, external partnerships, and in some cases migration or flexible talent pathways.

Recommended actions

Australian organisations should adopt a structured stress-test of their workforce planning using current labour-market data, explicit AI scenarios, and cross-functional governance involving HR, risk, technology, and strategy leaders. They should also benchmark elements of their approach against stronger international practice, particularly Singapore's integrated coordination, Saudi Arabia's strategic direction-setting, and Canada's sector planning models.

For boards and senior executives, the immediate goal is not to replicate another country's system but to ask sharper questions, identify capability gaps earlier, and align workforce decisions with the organisation's future risk environment. The accompanying checklist can support this process.

AI–Cyber Workforce Planning Stress-Test Checklist

This checklist is designed for boards, executive teams, senior public servants, and program leaders who need to assess whether current workforce planning is fit for AI-driven changes in cyber risk, governance, and capability demand.

Foundation

- Is there a current workforce plan that explicitly addresses AI and cyber risk, rather than referring only to general digital capability?
- Has the board or executive committee reviewed this plan within the last 12 months?
- Is there a clearly designated executive owner for AI- and cyber-related workforce planning?

Data and forecasting

- Does planning use current labour-market and sector data rather than relying only on historic staffing trends?
- Does the organisation model demand over a three- to five-year horizon?
- Have multiple scenarios been considered, including accelerated AI adoption and AI-enabled threat escalation?
-

Roles and capabilities

- Have critical hybrid roles been identified, including positions that combine cyber, AI governance, data, policy, and risk functions?
- Are role profiles and capability expectations defined for those positions?
- Is there a plan for redesigning work as AI tools automate or augment existing tasks?

Pathways and pipelines

- Are there clear pathways for building or acquiring talent, such as graduate recruitment, partnerships, reskilling, or specialist hiring?
- Has the organisation identified which capabilities must be built internally and which can be sourced externally?
- Has the organisation examined international examples of skills pipelines or external talent use, such as Singapore's coordinated labour-market model?

Governance

- Is workforce planning integrated into strategy and risk processes rather than treated as a standalone HR activity?[cite:21][cite:24][cite:31]
- Does senior leadership receive regular reporting on AI- and cyber-related capability gaps?[cite:21][cite:24]
- Is there cross-functional governance involving HR, technology, risk, operations, and policy teams?[cite:21][cite:24]

Benchmarking and review

- Has the organisation benchmarked its approach against relevant international practice, including Singapore, Saudi Arabia, or Canada?
- Is the workforce plan reviewed and updated as labour-market conditions, threat conditions, and AI adoption change?
- Are leaders participating in relevant education, policy, or professional networks to stay current on workforce-planning practice?

Simple rating scale

Use the following rating scale for each item:

- Green: in place and reviewed regularly.
- Amber: partly in place or inconsistently applied.
- Red: not in place or not evidenced.

Items rated amber or red should become priorities for executive discussion and follow-up action.