White paper

Freeing public security and networking talent to do more with automation

verizon business

Introduction

The rise of hyper-automation in Australia's public sector security and networking agencies marks a new chapter of opportunity. Building on past technological advancements that transformed how we live, work and connect, artificial intelligence (AI) is poised to unlock efficiencies and boost productivity like never before.

To enable a fair and inclusive future, however, pursuing these technologies with careful consideration of their impact on the workforce and society is essential. Governments worldwide are challenging themselves to craft new AI Bills of Rights to help talent thrive in the age of automation.[1, 2]

The Australian Government has released a consultation paper proposing mandatory safeguards for AI in high-risk contexts. The document details outlines proposed options for mandatory guardrails as preventative measures, requiring those developing and implementing high-risk AI to undertake specific actions throughout the AI lifecycle.[3]

These frameworks are crucial to counter fears of a "jobless future," as the World Economic Forum indicates that 22 percent of global jobs are expected to be fundamentally changed by 2030 as a result of technological change.[4]

The government's annual efficiency dividend, which mandates agencies to identify cost savings and productivity improvements equivalent to a specified percentage of their operating budgets (typically set between 1-2%), has come under scrutiny. [5] Labor's plan to save $6.4 billion over four years by reducing the use of consultants and external labor, potentially yielding up to $2 billion annually in savings, has been criticised by former public service commissioner Andrew Podger. He argues that the approach of increasing the efficiency dividend on administrative expenses is a "lazy option" that risks reducing service levels, causing longer wait times, and potentially leading to staff cuts and job losses.[6]

Driving down public spending through dividends—amplified by automation—carries risks if not underpinned by thoughtful governance and a desire to unleash human potential and productivity in the security and networking arena.

In particular, this risk applies to the Australian public defence sector, which employs approximately 19,500 public servants, supported by an outsourced civilian workforce estimated at over 30,000 contractors.[7] They carry the critical responsibility of securing Australia's cyber borders, with the average cost of a breach reaching $4.26 million and the number of notifications rising by 9% from the previous six months in 2024.[8]

The opportunity now presents itself to make Australia a world leader in security and networking talent, not by replacing humans with AI-driven automation but by amplifying their decision-making skills at scale with these emerging technologies guided by global standards and local regulations that prioritise human oversight and societal benefit.

Society 5.0 lights up the public sector horizon

Unlocking value in the public sector at scale with the same vigour as private companies is the holy grail of future societies, typified by Japan. Society 5.0 calls for a human-centred society that balances economic advancement with resolving problems in a system stretching across cyberspace and physical space.[9]

"People, things and systems are all connected in cyberspace, and optimal results obtained by AI exceeding the capabilities of humans are fed back to physical space. This process brings new value to industry and society in ways not previously possible," said the Japanese Cabinet Office.[9]

Australia must adopt similar long-term thinking, fostering innovation in the public sector while ensuring technology serves the needs of citizens, in line with the human-centric principles of Society 5.0.

The future security and networking workforce depends on digital transformation that spans government agencies and outsourced contractors, including sovereign primes.

Job roles with process-orientated or data-capture functions face potential automation through machine learning algorithms.

Prone to human error, these repetitive, time-consuming tasks can often be handled more efficiently by AI. While it's conceivable that up to 10% of the workforce may vanish, creative, rewarding new roles will emerge in the automation age. "Yesterday's secretaries are today's database administrators. Yesterday's milkmen are today's Uber Drivers," said Public Sector People.[10]

Plus, a security workforce armed with machines and intelligent software algorithms is more productive than one without them, reducing overall costs. "More broadly, workers who can complement the new automation, and perform tasks beyond the abilities of machines, often enjoy rising compensation," said the Brookings Institute. It moves the needle beyond the political shackles of the efficiency dividend, linking productivity to wages for the first time in history and giving Australia a digital edge in the AI age.[11]

> "More broadly, workers who can complement the new automation, and perform tasks beyond the abilities of machines, often enjoy rising compensation."[11]

People—not algorithms—first

While less visionary than the ideals of Japan's Society 5.0, Australia is showing a growing commitment toward building the world's best public service through the Digital and Customer Capability Framework. Designed by the NSW Public Sector Commission, it focuses on creating a long-term lean infrastructure powered by entrepreneurial AI disruption.

Processes are subordinate to people, and applications are customer-centric.[12]

At its core, the leadership model aims to empower security and networking talent by upskilling their digital literacy and supporting their decision-making with big data applications that reduce cyber risk and enable creative, critical thinking. The pilot Learning Experience Platform (LXP) is a tangible manifestation of the ecosystem to attract, develop and retain a responsive and capable workforce in the age of automation.

While both initiatives share a similar goal of leveraging technology to create more efficient and effective services, Society 5.0 has a broader scope and vision for transforming society. At the same time, the NSW Digital and Customer Capability Framework are more focused on developing specific skills and capabilities within the public sector.

> “At its core, the leadership model aims to empower security and networking talent by upskilling their digital literacy and supporting their decision-making with big data applications that reduce cyber risk and enable creative, critical thinking.”

Reaching for higher standards

Building a "super smart" society where security and networking professionals leverage AI, big data and the power of self-optimising plants under Industry 4.0 to drive enhanced decision-making requires a range of global standards to manage and secure the digital ecosystem. The concept of trust shines at the centre of these standards across both public and private sectors, especially as computing moves to the edge through Internet of Things (IoT) devices. They are also necessary to support governance considerations in a future society driven by technological change, including protecting sensitive customer and employee data, especially when they cross national borders.

Strategically, the zero trust network (ZTN) is a framework or philosophy which governs several global standards:

Assume that all users, devices and applications are untrusted. Access is granted only after verification, stressing the critical importance of continuous monitoring and risk assessment. [13]

Tactically, the standards that matter most to the next generation of cyber professionals fall below and support the ZTN. It's worth briefly summarising their purpose and framework.

- IS027001:2 is a standard that outlines the need for an information security management system (ISMS) while managing and protecting sensitive information [14]
- PCI Security Standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data.[15]
- CSF is a framework pioneered by the National Institute of Standards and Technology (NIST) to tackle cybersecurity risks and protect against cyber threats [16]
- NIST SO800-53 is a set of security controls and guidelines developed by NIST to help federal agencies and organisations protect their information and systems [17]
- The CSA Cloud Control Matrix is a framework for evaluating and managing security risks associated with cloud computing [18]
- The Cybersecurity Capability Maturity Model is a framework for assessing an organisation's cybersecurity capabilities and maturity [19]
- COBIT provides an IT governance and management framework that helps organisations align their IT strategies with business goals and objectives [20]

The strategic and tactical alliance between ZTN and the supporting standards enables digital transformation with a 'secure by design' approach for distributed teams and networking solutions. Public and private stakeholders are partnering on a range of cross-sector applications built on these standards that feature under the Digital and Customer Capability Framework or, more broadly, under Society 5.0, touching on cyber security, IoT, cryptocurrency and blockchain.

Ensuring Australian citizens trust technology driving the public service ecosystem and allied private sector applications requires robust principles and standards centred on data privacy and secure global data transfer protocols, prioritising how data is protected.

In particular, established principles and standards promote a society where users are empowered to manage their personal data and its use, including accessing government services like MyGov online, linked to Medicare, Centrelink and Child Support.

The Australian Privacy Act, for instance, governs the collection and use of personal data and provides the necessary protection through appropriate control mechanisms.[21]

The Australian Government has initiated a further review of the Privacy Act to align it with other globally recognised frameworks, including mandatory data breach reporting requirements to report a data breach, especially in light of the shocking new data revealing 40 large-scale data breaches towards the end of last year.[22]

Some of Australia's highest-profile organisations have experienced significant cyberattacks, impacting customers and tens of millions of end-users. In some cases, identification numbers attached to medical records highlighted how cybersecurity crosses public and private sectors in a digital society.

Preventing these attacks, especially in smaller entities with fewer resources than these larger organisations, is the goal of the Australian Cyber Security Centre's (ACSC) Essential Eight Maturity Model, which attempts to provide a consistent baseline from which to approach the philosophy of ZTN and data privacy in its operations. The model aims to simplify the landscape for security professionals and give them a visible, structured route towards securing digital transformation. Focusing on protecting Microsoft Windows-based internet-connected networks gives companies three maturity models to align their cyber operations.[23]

Increasingly, these models, including broader mitigation strategies falling under ACSC's Information Security Manual (ISM), and their adoption will separate innovators from laggards in the public sector, making their digital operations more transparent.[24]

Securing mission-critical infrastructure

These higher global and local standards, models and frameworks also reflect the growing digitisation of national infrastructure and the cyberattack surfaces that come with it. Consequently, the Australian Government introduced a series of legislative measures in 2024 to bolster the security of the critical infrastructure sector, especially in the aftermath of attacks against critical infrastructure in the US.

These measures encompass the Cyber Security Legislative Package, which includes the Cyber Security Act 2024, the Intelligence Services and Other Legislation Amendment (Cyber Security) Act 2024, and the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024 (ERP Act). Key obligations under these acts include mandatory ransomware reporting requirements and the establishment of a critical infrastructure risk management programme.

These incidents showcase to APAC governments the growing cyber vulnerabilities that may exist in public and private sector supply chains. They also revealed imperfect adherence to ZTN principles, further influencing the direction of new legislation. While previously, only education, food, transportation and energy appeared in the Security of Critical Infrastructure Act 2018 it now covers other verticals, including data storage, data processing and communications.[25]

Hyperscaling human potential

Technology leaders like Verizon, who deliver robust and scalable computing infrastructure, estimate that humans may account for 65% of all cyber breaches due to mistakes[26], misconfigurations or credential violations. Verizon's Security Orchestration, Automation and Response (SOAR) solution tackles this by enhancing human operations to minimise errors across both Information Technology (IT) and Operational Technology (OT) environments critical to industry configurations.

The centralised dashboard frees up security and networking analysts to view and manage security alerts from various sources in an organised, streamlined manner. Faster, informed decision-making is possible with a platform powered by machine learning algorithms. Under this framework, humans can quickly identify and prioritise alerts, automate incident response workflows and provide real-time visibility into security incidents, particularly for infrastructure categorised as mission-critical.[27]

> "Some of Australia's highest-profile organisations have experienced significant cyberattacks, impacting customers and tens of millions of end users."

Federal cyber hubs: a key to the golden age of public service

The Digital and Customer Capability Framework explicitly acknowledges that building a human-centric digital society and making Australia a world leader in public sector services will hinge on an always-on strategy to win the war on attracting and keeping cyber talent for building new government infrastructure and applications. In this context, talent will be motivated by more than wages.

Their work must serve the communities they live in and align with the ideals of the United Nations' 17 Sustainable Development Goals (SDG). Federal hub agencies like the DTA, ASD and the Australian Cyber Security Centre (ACSC) are essential in conveying these ideals, strategies, tactics, technologies and standards.

The opportunity to enter a golden age of public service has arrived, which will make government professionals the envy of their private sector peers. It also ushers in best-in-class public-private partnerships between global and sovereign primes that offer managed security and hosting solutions. In many cases, private technology leaders like Verizon may deliver trusted solutions to federal agencies.

Linking productivity to wages through automation

The Australian Government's "Future Made in Australia" initiative recognises that automation can drive both economic growth and job opportunities. By supporting skills development for automation in sectors like renewable energy, this strategy aims to enhance productivity whilst fostering secure, well-paid jobs, ensuring workers share in the economic prosperity. For example, its $91 million investment in developing a clean energy workforce will provide training in automation technologies for renewable energy sectors, directly linking enhanced productivity to higher wages and shared economic prosperity for workers, as outlined in the 2024-25 Budget.[28]

Digital and Customer Capability Framework and Society 5.0 confirms this long-term strategic thinking and needs, promising to finally let cyber talent earn competitive wages while growing the economy.

Ethics must drive an automated future

The ANU School of Cybernetics, led by Distinguished Professor Genevieve Bell, is focused on reimagining Cybernetics for the 21st century, bringing people together from different places, backgrounds and disciplines to build the safe technology of tomorrow.

The School describes an anthropological approach to complex systems involving people, machines, software and the surrounding environment. Professor Bell argues that leaders who genuinely encourage risk-taking are needed most in government right now to drive human-centred decision-making in the age of automation.[29]

The ANU School of Cybernetics is exploring regulatory reform and the risks of adopting AI-driven solutions too soon to drive efficiencies.

"As we negotiate these new contracts, questions inevitably arise about our relationships to the data that exists about us, the sheer abundance of information that we generate and how it could be used to help us or hurt us," Bell said.[30]

Conclusion

People, including public service security and networking talent, remain at the heart of digital transformation.

While government programs like the efficiency that comes with encouraging leaders to do more with less, cutting human talent to save costs will not make Australia a world leader in public service. Instead, automation can free up talent to think critically and decisively to benefit the communities they serve.

It's a golden opportunity for visionary leaders in public service to harness automation, enabled by key agencies and globally interoperable industry standards, to unlock scalable and critical human decision-making.

More than ever, fresh perspectives are needed to eliminate inefficiencies and superficiality from public service applications.

> "It's a golden opportunity for visionary leaders in public service to harness automation, enabled by key agencies and global and local standards, to unlock scalable and critical human decision-making."

Learn more

To learn more about future-ready public security sector automation, contact your Verizon Business Account Representative.

Email apaccontactus@verizon.com.
Visit verizon.com/business/en-au/contact-us/

References

1. United Nations. “Sustainable Development Goals.” https://www.un.org/sustainabledevelopment/sustainable-development-goals/

2. The White House. “AI Bill of Rights.” https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/

3. Australian Government Department of Industry, Science, Energy and Resources. “Mandatory guardrails for safe and responsible AI: have your say.” https://www.industry.gov.au/news/mandatory-guardrails-safe-and-responsible-ai-have-your-say

4. World Economic Forum. “The Future of Jobs Report 2025.” https://www.weforum.org/publications/the-future-of-jobs-report-2025/digest/

5. Australian Government Department of Finance. “Efficiency Dividend.” https://www.finance.gov.au/about-us/glossary/pgpa/term-efficiency-dividend

6. The Guardian. “Labor defends plan to save $6.4bn by cutting more consultants as experts call it a ‘lazy option” https://www.theguardian.com/australia-news/2025/apr/29/labor-defends-plan-to-save-64bn-by-cutting-more-consultants-as-experts-call-it-a-lazy-option

7. Australian Bureau of Statistics. “Public sector employment and earnings” https://www.abs.gov.au/statistics/labour/employment-and-unemployment/public-sector-employment-and-earnings/2023-24

8. IBM. “Cost of a Data Breach Report 2024.” https://www.ibm.com/reports/data-breach

9. Cabinet Office, Government of Japan. “Society 5.0.” https://www8.cao.go.jp/cstp/english/society5_0/index.html

10. Public Sector People. “Automation and the Future of Administrative and Business Support Roles within the Public Sector.” https://www.publicsectorpeople.com.au/automation-and-the-future-of-administrative-and-business-support-roles-within-the-public-sector

11. Brookings Institution. “Understanding the Impact of Automation on Workers, Jobs, and Wages.” https://www.brookings.edu/articles/understanding-the-impact-of-automation-on-workers-jobs-and-wages/

12. Public Service Commission NSW. “Building a Digital and Customer-Capable Workforce.” https://www.psc.nsw.gov.au/building-a-digital-and-customer-capable-workforce

13. Cloud Security Alliance. “Achieving Zero Trust Remote Access with Privileged Access Management.” https://cloudsecurityalliance.org/blog/2021/11/19/achieving-zero-trust-remote-access-with-privileged-access-management/

14. International Organization for Standardization. “ISO/IEC 27001: Information Security.” https://www.iso. org/isoiec-27001

15. PCI Security Standards Council. “PCI DSS v3.2.1 Quick Reference Guide” https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

16. National Institute of Standards and Technology. “Concept Paper: Cybersecurity Framework (CSF) 2.0.” https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf

17. National Institute of Standards and Technology. “Security and Privacy Controls for Information Systems and Organizations.” https://csrc.nist.rip/csrc/media/projects/risk-management/800-53%20downloads/800-53r5/sp_800-53_v5_1-derived-oscal.pdf

18. Cloud Security Alliance. “Cloud Controls Matrix.” https:// cloudsecurityalliance.org/research/cloud-controls-matrix/

19. US Department of Energy. “Cybersecurity Capability Maturity Model (C2M2).” https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

20. ISACA. “COBIT.” https://www.isaca.org/resources/cobit

21. Office of the Australian Information Commissioner. “Australian Privacy Principles.” https://www.oaic.gov.au/privacy/australian-privacy-principles

22. VMware. “How Data Privacy and Sovereignty Impact Business.” https://www.cio.com/article/474688/how-data-privacy-and-sovereignty-impact-business.html

23. Australian Cyber Security Centre. “Essential Eight Maturity Model.” https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eight/essential-eight-maturity-model

24. Australian Cyber Security Centre. “Information Security Manual (ISM).”https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism

25. Critical Infrastructure Centre. “Critical Infrastructure.” https://www.nationalsecurity.gov.au/protect-your-business/critical-infrastructure

26. Verizon. “2025 DBIR” https://www.verizon.com/business/en-au/resources/reports/dbir

27. Verizon. “Securing Critical Infrastructure.” https://www.verizon.com/business/resources/reports/securing-critical-infrastructure.pdf

28. Australian Unions. “Ed Husic on Automation and the World of Work. https://www.australianunions.org.au/podcast/ed-husic-on-automation-and-the-world-of-work/

29. Ministers for the Department of Industry, Science and Resources. “Discussion at the Australian Financial Review Workforce Summit.”https://www.minister.industry.gov.au/ministers/husic/transcripts/discussion-australian-financial-review-workforce-summit

30. Australian National University. “Who Is Building, Managing, and Decommissioning Our Technology-Enabled Future?” https://cybernetics.anu.edu.au/#who-is-building-managing-and-decommissioning-our-technology-enabled-future-1