Freeing public security and networking talent to do more with automation.

verizon business

Introduction

The arrival of hyper-automation in Australia's public security sector presents opportunities and challenges. While previous waves of technological change led to disruption in the way we live, work and play including unintended consequences such as job losses and wage stagnation, experts believe artificial intelligence (AI) can unlock new efficiencies and drive productivity.

To ensure a fair and inclusive future, however, pursuing these technologies with careful consideration of their impact on the workforce and society is essential. While the United Nations' 17 Sustainable Development Goals (SDGs) ambitiously address global concerns, including sustainable employment and decent work for all, governments worldwide are challenging themselves to craft new AI Bills or Rights to help talent thrive in the age of automation.[1] [2]

Australia is no exception, launching its 8 Artificial Intelligence Ethics Principles that seek to augment, complement and empower human cognitive, social and cultural skills, including security and networking talent.[3] These frameworks are crucial to counter fears of a "jobless future", as some studies suggest that automation may kill 30% of all jobs by the year 2030 from a global perspective.[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] Despite potentially resulting in up to A$2 billion in savings per year, critics argue that forcing agencies to do more with less can lower service quality, longer wait times and lead to staff cuts and job losses.[6]

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

In particular, this risk applies to the public defence sector, which employs around 17,400 public servants, augmented by an outsourced civilian workforce of over 28,000 contractors. [7] They carry the critical responsibility of securing Australia's cyber borders, with the average cost of a breach over $3 million and increasing in number by almost 10% each year.[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 ethical principles, global standards

Society 5.0 lights up the public sector horizon.

Unlocking value in the public sector at a faster, sustainable scale with the same vigour as private companies is the holy grail of future societies, including Asia Pacific neighbour Japan. Rather than relying upon automation for its own sake, imaginative new thinking under new initiatives labelled Society 5.0 is emerging.[9]

Society 5.0 calls for a human-centred society that balances economic advancement with resolving social problems in a system that stretches across cyberspace and physical space.[10]

"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.

Australia must adopt similar long-term thinking, driving innovation in the public sector while nurturing and encouraging diversity, equity and inclusion (DEI), typical of Society 5.0.

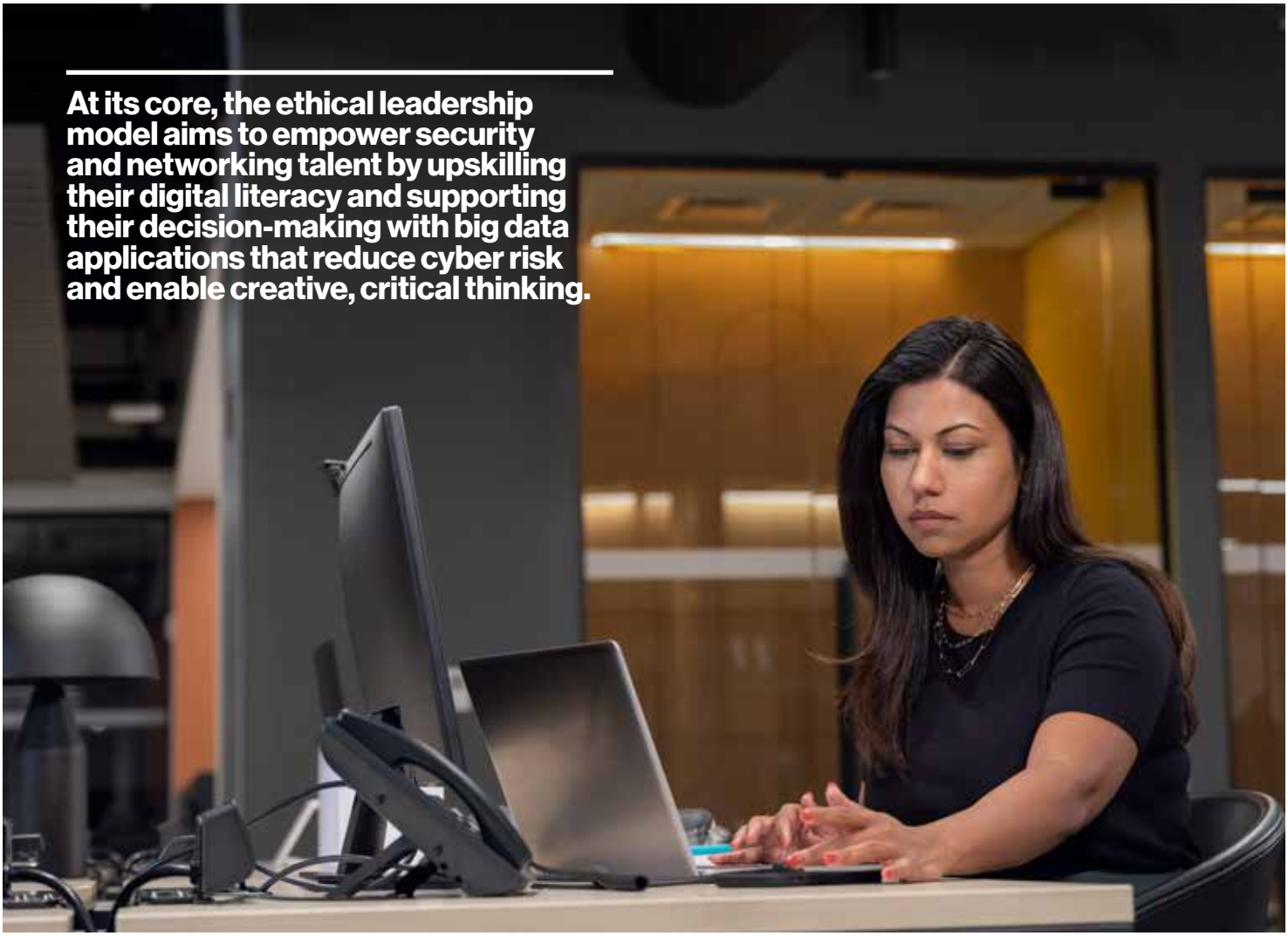
The future security and networking workforce depends on digital transformation that spans government agencies and outsourced contractors, including sovereign primes. Job roles with process-orientated or data-capture functions face inevitable automation through machine learning algorithms. Prone to human error, these repetitive, time-consuming tasks can 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.[11]

Plus, a security workforce armed with machines and intelligent software algorithms is more productive than those 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.[12]

There is also a growing consensus that Australia may need more digital security and networking talent by 2030 than currently anticipated. The Commonwealth Scientific and Industrial Research Organisation (CSIRO) estimates that 160,000 specialist AI workers will be required to build and supervise a wave of new automation technologies that form part of Society 5.0.[13]

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

People - not algorithms - first.



While less visionary than the ideals of Japan's Society 5.0, Australia is showing a growing commitment towards 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. In this ecosystem, processes are subordinate to people, and applications are customer-centric.[14]

At its core, the ethical 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.

Reaching for higher standards.

Building a “super smart” society where security and networking professionals leverage AI, Big Data, and the power of self-optimizing 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 ethical 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. [15]

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 needs for an information security management system (ISMS), while managing and protecting sensitive information [16]
- PCI is a set of security standards developed by the payment card industry to ensure that merchants who accept credit card payments maintain a secure environment [17]
- CSF is a framework pioneered by the National Institute of Standards and Technology (NIST) to tackle cybersecurity risks and protect against cyber threats [18]
- 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 [19]
- The CSA Cloud Control Matrix is a framework for evaluating and managing security risks associated with cloud computing [20]
- The Cybersecurity Capability Maturity Model is a framework for assessing an organisation’s cybersecurity capabilities and maturity [21]
- COBIT provides a IT governance and management framework that helps organizations align their IT strategies with business goals and objectives [22]

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 further supporting principles and standards around data privacy and sovereign data centres.

In particular, it calls for higher ethical standards in a society allowing users to control their digital destiny - including personal data - and how it is used, 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 for the necessary protection through appropriate control mechanisms.[23]

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.[25] [26]

Some of Australia's highest-profile organisations have experienced significant cyber-attacks, impacting customers and end-users numbered in the tens of millions. In some cases, identification numbers attached to medical records highlighted how cyber security crosses the 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.[28]

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.[29]

Some of Australia's highest-profile organisations have experienced significant cyber-attacks, impacting customers and end-users numbered in the tens of millions.

Securing mission-critical infrastructure.

These higher global and local standards, models and frameworks above also reflect the growing digitisation of national infrastructure and the cyber-attack surfaces that come with it. Consequently, new Australian legislation aims to broaden the scope of mission-critical infrastructure, especially after the debilitating aftermath of attacks against critical infrastructure in the US. These incidents showcase to the APAC governments the growing cyber vulnerabilities that now exist in public and private sector supply chains, and revealed a weak adherence to ZTN principles, further influencing the direction of new legislation. While previously, only education, food, transportation and energy appeared in the bill, it now covers other verticals, including data storage, data processing, and communications.[30]

Hyperscaling human potential.

Hyperscalers like Verizon, providing large-scale, highly available, and scalable computing infrastructure, estimate that humans may account for 85% of all cyber breaches due to mistakes, misconfigurations or violations involving credentials. Verizon's Security Orchestration, Automation and Response (SOAR) solution addresses this challenge by augmenting human operations to reduce errors across both Information Technology (IT) and Operational Technology (OT) that feature prominently in 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.[31]

Strategic certification for secure public operations.

The Digital Transformation Agency (DTA) also allows multinational companies like Verizon to certify their hosting security controls compliant with the mission-critical infrastructure encompassing public sector supply chains and data and systems. The Australian government can select from a range of 'Certified Strategic' cloud service providers with the highest degree of confidence that its choice(s) is secure in dealing with the emerging cyber threat landscapes for its customers and citizens. It also allows security and networking professionals to operate confidently on emerging projects based on existing compliance and global standards.[32]

Secure connectivity gateways (SIGs) in a digital society.

The DTA often joins other agencies, including the Australian Signals Directorate (ASD), to enhance security at the meeting point between government agency networks and the public internet. Enhancing protective barriers form part of the government mission (and Cyber Hub Initiative) to "create a secure online world for Australians, their businesses and the essential services on which we depend".[33]

The above shows a renewed intent to modernise gateways against growing cyber threats locally and abroad with the next generation of Certified Australian Gateway Environments (CAGE)-compliant SIGs. Blocking non-essential internet traffic needs constant algorithmic supervision, repelling cyber-attacks while limiting security incidents. Higher gateway security helps networking and security professionals with intelligent decision-making to benefit all public sector customers.[34]

Future-proofing public sector with diversity.

"The recent pandemic was a dress rehearsal for the next ten years, from a technology perspective," said Rob Le Busque, Vice President for APAC, Verizon Business.

Intense competition for cyber talent on the corporate battlefield requires a new generation of diverse problem solvers. Pursuing frictionless global trade environments and building a digital society of the future requires renewed energy and focus on Diversity, Equity and Inclusion (DEI).

Rob comments that overcoming virtue signalling and unconscious bias when building or upgrading new technology platforms in the public sector is critical to ensure all Australians, even those with disabilities, can access secure, easy-to-use systems in a world approaching Society 5.0. It also moves the public sector beyond brute strength security and networking systems, enabling more diverse hiring practices.[38]

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 needs to service the communities they live in and strive for the ideals of the United Nations' 17 SDG goals. 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 hyperscalers like Verizon may deliver trusted solutions to up to 90 federal agencies.

Linking productivity to wages through automation - for all.

"Technology has often been good for profits but bad for jobs. It should be good for both - and can be," said Hon Ed Husic MP, Minister for Industry and Science. "Productivity and wages remain intimately linked. If we're serious about technology, we need a long-term strategy to share economic prosperity with staff and workers." [39]

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. Further, it ensures those previously marginalised groups in Australia can now pursue public sector positions and share in Australia's digitally-driven wealth.[40]

Ethics must drive an automated future.

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

"Cybernetics is being reimagined for the 21st Century as an essential tool for navigating major societal transformations through capability building, policy development and safe, sustainable, and responsible approaches to new systems," said the school.[41]

It describes an anthropological approach to complex systems involving people, machines, software and the surrounding environment. Prof Bell argues that leaders who genuinely encourage risk-taking are needed most in government right now to drive ethics and human-centred decision-making in the age of automation.[42]

It's also exploring regulatory reforms 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," said Prof Bell.[43]

Conclusion

The arrival of hyper-automation in Australia's public security sector presents In the age of hyperscaling and hyper-automation, the government must aim for the ideals and planetary goals outlined by the United Nations, Society 5.0, and the Digital and Customer Capability Framework.

People, including public service security and networking talent, remain at the heart of digital transformation and Australia's effort to build a sustainable, equitable digital society.

While government programs like the efficiency dividend encourage 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 unlock diverse scalable, critical human decision-making on a wave of automation made possible by key agencies and global and local standards.

More than ever, diverse thinking is needed to remove unconscious bias and virtue signalling from public service applications.

It's a golden opportunity for visionary leaders in public service to unlock diverse scalable, critical human decision-making on a wave of automation made possible by key agencies and global and local standards.

References

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

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

3. Australian Government Department of Industry, Science, Energy and Resources. “Australia’s AI Ethics Principles.” https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-framework/australias-ai-ethics-principles

4. Public Sector People. “Automation and the Future of Administrative and Business Support Roles within the Public Sector.” https://www.publicsectorpeople.com.au/blog/2022/09/automation-and-the-future-of-administrative-and-business-support-roles-within-the-public-sector?source=google.com

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

6. ABC News. “Coalition Costings Reveal Public Sector Cuts, More Contractors.” https://www.abc.net.au/news/2022-05-17/cuts-public-sector-spending-coalition-policy-costings-election/101072270

7. ABC News. “Contractors and the Public Service: Is the Gig Economy Taking Over?” https://www.abc.net.au/news/2020-09-10/contractors-and-the-public-service-gig-economy/12647956

8. Hit Network. “Australia to Establish New National Office Tackling Cyber Security.” https://hit.com.au/story/australia-to-establish-new-national-office-tackling-cyber-security-215142

9. Australian National University. “Security Society 5.0.” https://sdsc.bellschool.anu.edu.au/news-events/news/6957/security-society-50

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

11. Public Sector People. “Automation and the Future of Administrative and Business Support Roles within the Public Sector.” https://www.publicsectorpeople.com.au/blog/2022/09/automation-and-the-future-of-administrative-and-business-support-roles-within-the-public-sector?source=google.com

12. Brookings Institution. “Understanding the Impact of Automation on Workers, Jobs, and Wages.” https://www.brookings.edu/blog/up-front/2022/01/19/understanding-the-impact-of-automation-on-workers-jobs-and-wages/#:~:text=Automation%2C%20jobs%2C%20and%20wages&text=Workers%20who%20can%20work%20with,the%20creation%20of%20new%20jobs.

13. CSIRO. “CSIRO Brokers New Partnerships to Foster Tech Talent.” https://www.csiro.au/en/news/news-releases/2022/csiro-brokers-new-partnerships-to-foster-tech-talent

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

15. 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/

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

17. Australian Cyber Security Centre. “Quick Wins for Your Website.” https://www.cyber.gov.au/sites/default/files/2021-11/Attachment_A_%20ACSC-Quick_Wins-for-your-website_V6.pdf

18. 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

19. National Institute of Standards and Technology. “Security and Privacy Controls for Information Systems and Organizations.” https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

References

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

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

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

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

24. VMware. “How Data Privacy and Sovereignty Impact Business.” https://blogs.vmware.com/cloud/2022/08/04/how-data-privacy-and-sovereignty-impact-business/

25. HWL Ebsworth Lawyers. “Catching Up with International Developments in Privacy: The Commonwealth’s Privacy Act Review 2022.” https://hwlebsworth.com.au/catching-up-with-international-developments-in-privacy-the-commonwealths-privacy-act-review-2022/

26. ABC News. “Data Breaches Revealed by Australian Information Commissioner.” https://www.abc.net.au/news/2023-03-01/data-breaches-revealed-by-australian-information-commissioner/102039710

27. BBC News. “Australia’s Critical Infrastructure Protection Agency Defends Itself Against ‘Flood’ of Cyber-Attacks.” https://www.bbc.com/news/world-australia-63056838

28. Australian Cyber Security Centre. “Essential Eight Maturity Model.” https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

29. Australian Cyber Security Centre. “Information Security Manual (ISM).” https://www.cyber.gov.au/acsc/view-all-content/ism

30. Critical Infrastructure Centre. “Critical Infrastructure.” https://www.cisc.gov.au/legislative-information-and-reforms/critical-infrastructure

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

32. Australian Signals Directorate. “Hosting Certification Framework.” https://www.hostingcertification.gov.au/framework

33. Digital Transformation Agency. “Updates: Secure Internet Gateway.” https://www.dta.gov.au/news/updates-secure-internet-gateway

34. CSO Australia. “Totally Different Technology Helps Verizon Secure AFP $15m MSS Deal.” http://www2.cso.com.au/article/520450/_totally_different_technology_helps_verizon_secure_afp_15m_mss_deal/

35. InnovationAus. “Adobe Lands $32 Million MyGov Tech Contract.” https://www.innovationaus.com/adobe-lands-32-million-mygov-tech-contract/

36. IT News. “DTA to Live on within Services Australia.” https://www.itnews.com.au/news/dta-to-live-on-within-services-au

37. InnovationAus. “Bureaucratic Inertia the Biggest Barrier to Transformation.” https://www.innovationaus.com/bureaucratic-inertia-the-biggest-barrier-to-transformation/

38. 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/

39. 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

40. 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

41. Inspiring NSW. “A Point Through Time.” https://inspiringnsw.org.au/2022/12/12/a-point-through-time/

42. Australian National University Cybernetics. “Applying Cybernetics and Collective Intelligence to System Reform.” https://cybernetics.anu.edu.au/news/2023/02/27/Applying-cybernetics-and-collective-intelligence-to-system-reform/

43. MIT Technology Review. “We need mass surveillance to fight COVID-19 – but it doesn’t have to be creepy.” https://www.technologyreview.com/2020/04/12/999186/covid-19-contact-tracing-surveillance-data-privacy-anonymity/

verizon business

© 2023 Verizon. All rights reserved. The Verizon name and logo and all other names, logos and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners. 00/21