IT Professionals Australia

Submission to Australia's 2020 Cyber Security Strategy

ABOUT IT PROFESSIONALS AUSTRALIA

IT Professionals Australia represents ICT professionals across the full spectrum of industries and specialisations. Our members work in a wide variety of roles including ICT trainers, ICT sales, business and systems analysts, multimedia specialists, web developers, software and applications programmers, database and systems administration, ICT security, ICT support, test engineers, telecommunications and ICT management.

IT Professionals Australia is a division of Professionals Australia (formerly the Association of Professional Engineers, Scientists and Managers, Australia) which is an organisation registered under the Fair Work Act 2009 representing over 25,000 Professional Engineers, Professional Scientists, Veterinarians, Architects, Pharmacists, Information Technology Professionals, Managers, Transport Industry Professionals and Translating and Interpreting Professionals throughout Australia. Professionals Australia is the only industrial association representing exclusively the industrial and professional interests of these groups.

IT Professionals Australia
GPO Box 1272, Melbourne, Vic. 3001
e: info@professionalsaustralia.org.au
w: www.professionalsaustralia.org.au/information-technology/
t: 1300 273 762

CURRENT PERFORMANCE OF THE ICT INDUSTRY

The current rate of technological change occurring around the world is unparalleled throughout history. New technology is rapidly altering the way businesses operate, and the ability to incorporate new developments into existing businesses can be crucial in maintaining efficiency and boosting workplace productivity. It is estimated that the digital economy will be worth $139 billion by 2020 (7.3 per cent of GDP)[1]

Information and Communications Technology (ICT) is one of the top ten occupations which are projected to add the largest numbers of new jobs over the five years to May 2022. [2]The sector continues to strengthen and demand for IT professionals is set to improve further, with ICT driving business innovations through intelligent data analytics and information management systems, and organisations positioning themselves for cloud-based advancement. ICT in the form of telephony and the use of tablet devices continues to drive streamlined business practices and modernised service delivery in the telecommunications, business, education and training, retail and entertainment industries.

A recent report by Deloitte Access Economics found that employment in the number of ICT professionals is expected to grow from 663,100 workers in 2017 to 758,700 by 2023[3]. Despite strong growth, some challenges remain for local ICT professionals if they are to differentiate themselves amid the wider trends of offshoring and automation. In order for Australia to keep up with the demands of digital technology, local industries will need to successfully embrace new technology. Attracting and retaining skilled ICT professionals will be vital to this process.

The sector has performed relatively strongly over the past five years, buoyed by the rapid adoption of new technologies within businesses. According to industry research firm IBISWorld, revenue in IT consulting has increased by an annualised 3.0 per cent over the 5 years through 2019.[4] ICT professionals operate in a wide range of industries outside direct consulting, however the performance of this industry serves as a close proxy, highlighting the rising demand for ICT services throughout the economy more generally. While revenue has grown significantly, the number of employees in IT consulting has also grown strongly, rising by 2.0 per cent.[5] This growth reflects the rising uptake of ICT services, and the need for businesses to optimise their ICT operations and innovate.

Submission to Australia's 2020 Cyber Security Strategy

Technological progress and effective interaction in cyberspace is a key driver of economic growth throughout Australia, and across the globe. The current rate of technological change is unparalleled, with technological advancement driving major change across industries and throughout the ICT workforce. The internet is the key component in delivering essential services, connecting families, friends and workplaces, necessitating a balanced and effective cyber security strategy.

New technology is altering the way businesses and our society operate, with innovation and cutting-edge developments crucial to greater efficiency, improved workplace productivity and a better bottom line.

Australia's modern cyber security capability depends on its technological edge, yet technology alone cannot achieve our nation's security. It is people - their knowledge, what they create and how they innovate - that shapes the development, operation and future of our security online.

The responsiveness and capacity of our cyber security institutions is fundamentally underpinned by the knowledge and expertise of the ICT, engineering, science and technical workforce - the people who develop, select, integrate, maintain and operate our modern cyber security effort. The role of government and the Australian Public Service in this mission is fundamental.

To establish a foundation of effective cyber security, the Government must stop the erosion of ICT, science, engineering and technical expertise in the Australian Public Service by committing to a highly skilled and qualified APS technical and professional workforce, based on medium to long-term requirements.

If the Government is serious about its responsibilities to be an intelligent customer in the acquisition, sustainment and development of existing and emergent cyber security capability and infrastructure, then it needs to ensure it has a continuity of in-house ICT, science and engineering expertise.

RESPONSES TO SPECIFIC QUESTIONS POSED BY GOVERNMENT

What is your view of the cyber threat environment? What threats should Government be focusing on?

Until we pass the technological singularity, the foundational element in the cyber threat environment is the human in the system. The cyber threat environment is evolving in line with the unparalleled rate of technological change.

A complex systems approach will be critical for understanding threats into the future. Government and industry must also properly manage end of life systems sitting at the periphery of networks, such as ad-hoc IoT systems.

Do you agree with our understanding of who is responsible for managing cyber risks in the economy?

Governments and organisations are generally best placed to develop and instil systemic controls, where as individuals are best placed to manage and control their own behaviour or that of their families.

Risk should be handled by the person or organisation best positioned to control that risk, including consideration of institutional or individual technical capacity.

Do you think the way these responsibilities are currently allocated is right? What changes should we consider?

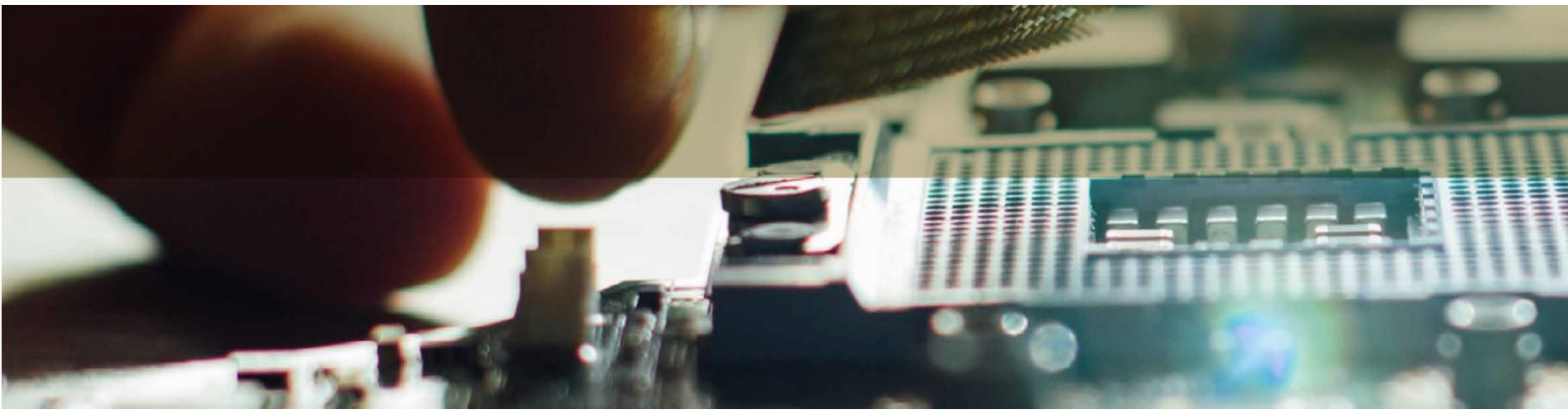
Increased data breach reporting would drive security. The Notifiable Data Breaches scheme (NDB scheme) introduced new obligations in 2018 for Government agencies and the private sector requiring them to notify individuals of eligible data breaches.

Transparency and accountability should underpin good privacy practice. The requirement to understand and be prepared to respond to data breaches drives organisations to think about, and develop plans to respond to, human and cyber data threats and breaches.

What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?

The Government is not as well placed as a leader in this area as it has been in the past. Years of staffing caps and outsourcing of technical work has resulted in a brain drain from public cyber security institutions. If the Government is serious about its responsibilities to be an intelligent cyber security leader, and an intelligent customer in the acquisition, sustainment and development of existing and emergent cyber security capability and infrastructure, then it needs to ensure it has a continuity of in-house ICT, science and engineering expertise.

The Government should also strengthen its reporting and response capabilities and explore



what barriers there are to using business insurance as another response/driver for improved business behaviour.

How can Government maintain trust from the Australian community when using its cyber security capabilities?

We would argue that trust must be restored and developed, rather than maintained.
As mentioned previously, transparency and accountability should underpin best practice. It is demonstrably clear that successive governments have become incredibly secretive regarding their cyber security capabilities.

Governments have also become fervent in taking action against whistle-blowers and media who speak out regarding alleged misuse of those capabilities. There must be an open and transparent discussion about what government does and does not do with its cyber security capabilities, and government must allow full public scrutiny of how it uses citizen data.

What customer protections should apply to the security of cyber goods and services?

Companies should demonstrate appropriate security patches to their software and make End User License Agreements readable and short so consumers can be more informed of their rights and responsibilities in using their products. Government should investigate options for sensible regulation in this space.

Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?

The Government has a responsibility to act as a leader in delivering essential services and in areas where action is essential but the market fails to respond due to unknown risk and very large consequences. The Government must continue its current leadership role and also rebuild inhouse technical capacity, while maintaining the current openness in the market.

Is the regulatory environment for cyber security appropriate? Why or why not?

Professionals Australia would argue that concerns about the effectiveness of the regulatory environment may be an issue with under-resourcing rather than regulation.

How could we approach instilling better trust in ICT supply chains?

Rather than looking at starting at the top of the manufacturing chain we should be looking at building foundational capabilities. For example, what is needed to nurture a 3D Printing manufacturing sector?

How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?

If Australia is to remain competitive in this period of rapid change, we require a highly skilled, vibrant local ICT workforce. ICT professionals have become a vital part of the corporate world, and both employment and remuneration in the profession have increased in recognition of the critical role ICT now plays in business innovation and analytics.

According to recent data from Deloitte, the number of ICT Professionals in Australia has risen to a record 640,846 in 2016, totalling 5.4% of the workforce. This figure is forecast to swell to 721,886 by 2022, reflecting the increasingly integral role of ICT in business transformation while also providing a raft of new opportunities for ICT professionals. A significant challenge is that we are paying domestic wages and conditions for expertise that is in global demand, and other countries and companies are willing to outbid domestic pay and conditions.

To create a more sustainable Australian IT labour market and address potential distortion created by the unique mix of skills, education levels and people that make it up, Professionals Australia sees a strong need to ensure that proper migrant wage protections are in place and enforced, that skilled migration visa programs sit alongside independent and up-to-date analysis of areas genuinely in shortage, that a level of secure work exists over and above insecure, short-term, project based positions

in the IT industry, that offshoring doesn't replace proper investment in the further training and development of local IT professionals and that initiatives are put in place to lift the participation rate and retention of women in the technical workforce.

What changes can Government make to create a hostile environment for malicious cyber actors?

This question needs to be balanced with our values - undermining encryption does expose some malicious actors but puts the broader community at risk that the vulnerability will be discovered. It also undermines our democratic traditions.

What private networks should be considered critical systems that need stronger cyber defences?

Most major networks are private. The internet is the key component in delivering essential services, connecting families, friends and workplaces, necessitating a balanced and effective cyber security strategy.

The banking and finance system, communications and energy systems are clearly critical. However wherever significant amounts of personal information reside should be considered a high value target by a malicious actor.

What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

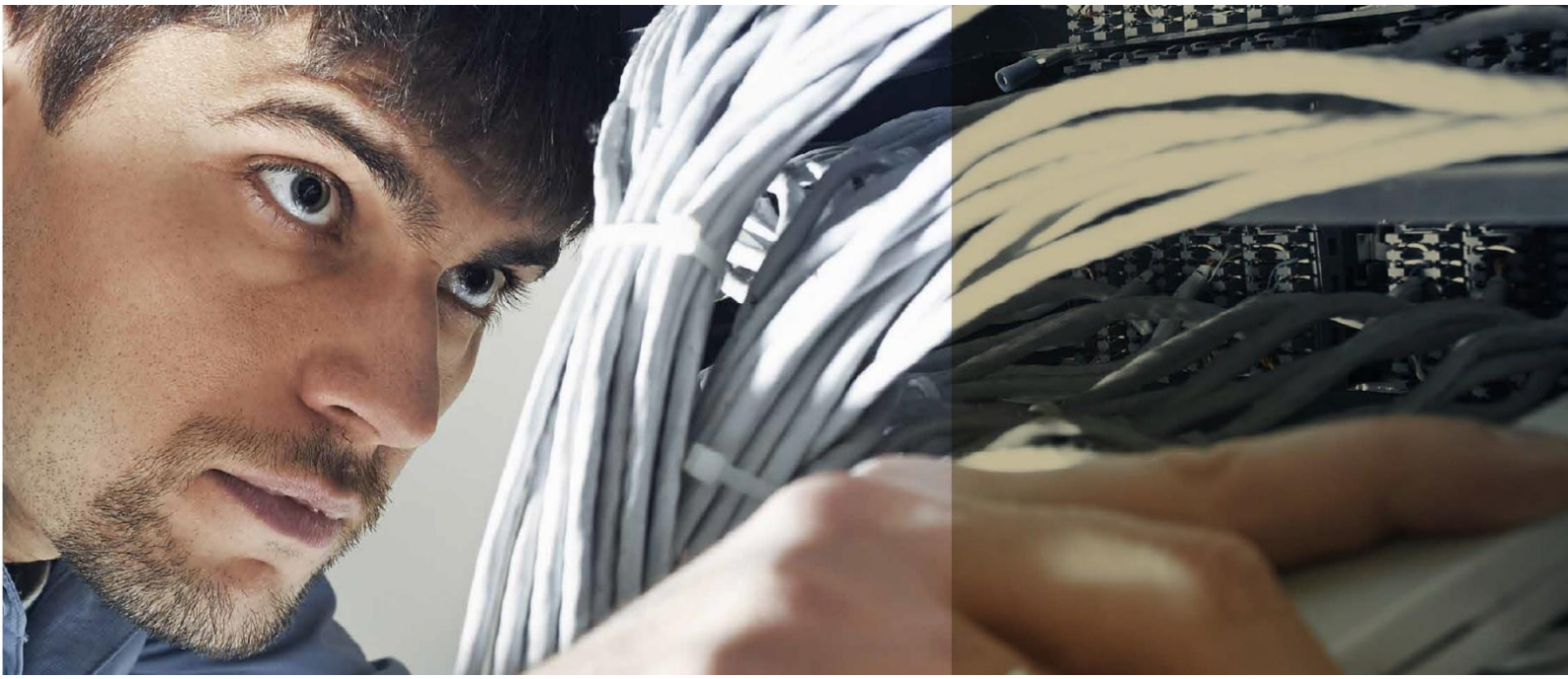
Some Professionals Australia members indicated concern that a regulated organisation will have the information they disclose used by the regulator.

To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

Agree, however awareness is not the only driver of poor consumer choice. In an environment where consumption of cyber content is virtually essential in daily life, price is also a significant factor.

What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?

The Australian Signals Directorate's Essential Eight Strategies to Mitigate Cyber Security Incidents. This prioritised list of mitigation strategies assists organisations in defending their systems against adversaries. The strategies are scalable and adaptable to organisations of different sizes and compositions.



IT Professionals Australia

Respect, recognition and reward

Submission to Australia's 2020 Cyber Security Strategy

STREET ADDRESS
152 Miller Street, West Melbourne,
Victoria, 3003, Australia

POSTAL ADDRESS
GPO Box 1272, Melbourne
Victoria 3001, Australia

TELEPHONE
1300 273 762

EMAIL
itpa@professionalsaustralia.org.au

WEB
www.professionalsaustralia.org.au/information-technology

Notes

1 Deloitte Access Economics, The Connected Continent II: How digital technology is transforming the Australian economy, 2015, p.1.

2 Department of Jobs and Small Business (2018). Australia Jobs 2018. Australia's 10 most-in-demand jobs revealed. Available at https://www.sbscom.au/yourlanguage/hindi/en/article/2018/07/23/australias-10-most-demand-jobs-revealed.

3 Deloitte Access Economics, Australia's Digital Pulse, 2018, p.3.

4 IBISWorld Industry Report M7000 Computer System Design Services in Australia, March 2019, p.4.

5 ibid, p.32 (Employment annual change).