AustCyber
Australian Cyber Security Growth Network

AUSTRALIA'S CYBER SECURITY SECTOR COMPETITIVENESS PLAN

2019 UPDATE

Driving growth and global competitiveness

PLAN AT A GLANCE

Purpose

To grow a vibrant and competitive cyber security sector, that generates increased investment and jobs for the Australian economy

Outlook

Global **demand** **surging**

US$145 billion on cyber security in 2018

86 **per cent increase** expected by 2026

Australia's **revenue from cyber security could triple** over the next decade

Australia well placed to become **global cyber security powerhouse**

Challenges being addressed

Skills shortage – around 17,000 more cyber security workers by 2026

Lack of alignment in research and commercialisation – need to concentrate on areas of strength and sector segments of software, security operations and underlying processes

Market barriers – need to remove hurdles so local companies can scale, mature and export solutions

Lack of robust measurement on impact and contribution to the economy – need data on the sector to support commercial decision making and track progress

Actions for growth

Coordinated investment and effort required across the cyber security industry, the research, education and training sector, and government to:

Grow the ecosystem

- Help startups find first customers
- Make access to seed and early-stage venture capital easier
- Improve research focus and collaborate to assist commercialisation
- Simplify government and private sector procurement processes
- Provide robust measurement of the ecosystem's development and impact on the Australian economy

Export to the world

- Support Australian companies to develop scalable service delivery models
- Attract multinationals to use Australia as base for reach into the Indo-Pacific region
- Develop cyber security as educational export

Lead in cyber education

- Attract and retain best and brightest
- Ramp up efforts to embed world leading cyber security education and training
- Create vibrant, industry-led professional development pathways

Benefits

✓ Thriving and dynamic, globally competitive cyber security sector

✓ New jobs and increased revenue

✓ Support for Australia's national security through effective, sovereign cyber security capability

✓ Foundation for future success of all industries across the economy through digitally driven growth

FOREWORD

Spending on cyber security worldwide is expected to soar over the next decade.

Cyber security is one of the most rapidly expanding sectors worldwide. Global spending on cyber security products and services is expected to increase by 88 per cent over the next eight years, from around US$145 billion today to almost US$270 billion in 2026. In Australia in 2018, external spending on cyber security products and services grew by eight per cent to A$3.9 billion. This compares with six per cent growth in 2017.

While Australia's cyber security sector is still developing, there is the potential to capture a significant share of the growing global cyber security market.

The sector is quickly growing in maturity and size, with an increasing number of home-grown success stories.

The 2019 update to Australia's Cyber Security Sector Competitiveness Plan again draws on extensive industry consultation and research to provide an updated picture of the global outlook, challenges, opportunities and priority actions needed to grow a vibrant and globally competitive cyber security sector that enhances Australia's future economic growth.

Last year's update provided a 'deep dive' on the skills and workforce gap – one of three key issues holding back the sector's growth. This year's deep dive explores the underlying structural challenges of not yet having robust measurement of the sector's development, as well as the economic impacts.

A clear view of the maturity and size of Australia's cyber security sector is essential for strategic growth. Good policy and future investments are contingent upon policymakers, entrepreneurs and investors having a clear picture of the sector on which to make informed decisions.

This problem of poor sector economic data is not unique to Australia. Currently, there are no robust and repeatable measurements of the cyber security sector in any country, meaning the economic characteristics of the cyber endeavour are poorly understood.

Cyber security as a business activity, as well as an economic pursuit, cuts across all many different sectors and industries. It includes not only providers of cyber security capability who comprise the cyber security sector, but also organisations in other sectors that employ in-house cyber security staff. Furthermore, cyber security products and services also protect and enable the infrastructure, supply chains and value chains of the digital aspects of the global economy, but the benefits of cyber security have not been studied to the necessary depth and richness.

Solving these measurement challenges will allow governments to form more robust and sophisticated industry development policies; encourage investment in the sector; and help cyber security companies to better understand their commercial surroundings and the opportunities available to them.

I hope the measurement of fundamental economic metrics such as the size of the sector and its value added to the economy can serve as a foundation to more sophisticated analysis – such as the broader impacts of cyber innovation across the economy, including its role as an enabler of growth and its beneficial impact to overall prosperity.

The 'Australian Cyber Security Industry Roadmap' continues to be a companion document to this Sector Competitiveness Plan to enable growth opportunities for Australia. Developed in partnership with CSIRO Futures, the Roadmap primarily focuses on the role of cyber security as a 'horizontal' and how it can enable growth opportunities in other sectors. Together, this plan and the roadmap are guiding documents for sector growth.

The past year has seen progress in several areas and Australia is in a strong position. But more needs to be done to ramp up the momentum over the next 12 months – including targeted government and industry investment in infrastructure to support commercialisation and innovation, and the establishment of a national platform for measurable and scalable cyber security skills development and workforce growth.

Key alignment opportunities will arise through the forthcoming national 2020 Cyber Security Strategy and the industry development strategies of state and territory governments, as well as coordinated efforts on behavioural norms for cyber space in international multilateral forums.

A globally competitive Australian cyber security sector will ultimately underpin the future success of every industry in the national economy. A consolidated effort is needed to continue to build on early successes and sustain Australia's competitiveness and strategic advantages in the creation and commercialisation of cyber security products and services.

Michelle Price
AustCyber Chief Executive Officer

> "
> Australia's cyber security sector has the potential to capture a significant share of the growing global cyber security market

ABOUT THIS PLAN

Plan structure

This plan is divided into six sections:

- ### Executive summary

- ### Chapter 1

  describes the **global outlook,** including the size and composition of the global cyber security sector, key demand forecasts underpinning the sector's rapid growth, and technological trends shaping the future pattern of demand across the sector's key market segments.

- ### Chapter 2

  describes the **potential growth opportunities for Australia**, including the three market segments that promise the steepest economic gains and warrant priority action: software; services to improve security of basic information technology (IT) and network infrastructure; and services focused on underlying processes (such as governance, risk and compliance, and training and awareness).

- ### Chapter 3

  describes the **challenges to sector growth**, focusing on four key issues: the impact of the skills shortage; barriers to innovation in the national research and commercialisation system; barriers to growth and exports; and the lack of robust measurement of the sector and its impacts across the economy.

- ### Chapter 4

  recommends **actions to build a more competitive cyber security sector**, including responsibilities for industry, government and the research, education and training sector. It also provides a **scorecard summarising progress on actions over the past 12 months** to advance Australia's cyber security sector, focusing on growing the ecosystem, increasing exports and becoming a leader in cyber security education.

- ### Chapter 5

  explains more about AustCyber, its mission, role in driving growth in the sector and strategic objectives to 2020.

- ### The Appendices

  provide **additional information** including Industry Knowledge Priorities that set out industry research needs and commercialisation opportunities for Australia's cyber security sector, methodologies and assumptions underpinning the findings in this plan and AustCyber's Regulatory Reform Plan.

Terminology

- **Cyber security sector** refers to all cyber security organisations and activities (including private sector, government, academia, research, training and education).

- **Cyber security industry** refers to private sector organisations and activities.

Background

The Australian Government's national **Cyber Security Strategy**, released in 2016 and backed by around $230 million of funding, elevated cyber security to an issue of national importance and led to the formation of the Australian Cyber Security Growth Network Ltd (AustCyber) at the beginning of 2017.

AustCyber is charged with leading the growth of Australia's cyber security sector – both as a trusted source of cyber security capability to organisations at home and abroad, and as an enabler for growth across the entire Australian economy. AustCyber recognises Australia's enormous opportunity in cyber security, as well as the urgency to act.

This Sector Competitiveness Plan provides a 10-year strategic outlook and vision for Australia to take its place as major cyber security exporter and world-leading hub for skilled cyber security talent. Together with AustCyber's other practical initiatives to support the industry, it aims to strengthen Australia's cyber security sector as a foundation for a digital business transformation and a catalyst for wider economic growth.

Acknowledgements

AGC Partners

Amadeus Capital Partners

Austrade, Australian Government

Australian Curriculum Assessment and Reporting Authority

Australia Defence Force Academy/University of New South Wales Canberra

Australian Energy Market Operator

Australian Federal Police, Australian Government

Australian Information Security Association

Australian Signals Directorate, Australian Government

Australian Unity

Box Hill Institute

BT Group

Canberra Institute of Technology

CBR Innovation Network

Cisco Systems

Cogito Group

Coles Supermarkets

Commonwealth Bank of Australia

CSIRO Data61

Deakin University

Decipher Bureau

Defence Science and Technology Group, Australian Government

Department of Education and Training, Australian Government

Department of Industry, Innovation and Science, Australian Government

Department of Finance, New South Wales Government

Department of the Prime Minister and Cabinet, Australian Government

Edith Cowan University

Hivint

IBM

icare

Intelligent Business Research Services

Kasada

KPMG

La Trobe University

Macquarie Telecom

Medibank Private

Nuix

Optus

QuintessenceLabs

Penten

PwC

Sapien Cyber

Secure Code Warrior

Security Innovation Network

Telstra

TAFENSW

University of New South Wales

Westpac

WithYouWithMe

> Cyber security
> is emerging as
> one of Australia's
> most promising
> growth sectors

CONTENTS

EXECUTIVE SUMMARY

Cyber security is emerging as one of Australia's most promising growth sectors

A surge in demand for cyber security products and services globally – driven by the growing need of organisations to protect their digital assets and databases from malicious activity – bodes well for Australian security companies.

Market trends point to tremendous economic opportunity. Global annual spending on cyber security increased by 10 per cent to US$145 billion in 2018 and is expected to remain robust in coming years. The outlook for cyber security spending in the Indo-Pacific region, which includes Australia's immediate Asia-Pacific neighbour states, as well as China and India, is particularly strong. Australia's innovative cyber security companies are gaining respect and success both at home and in international markets.

Cyber security is not only a dynamic sector offering a new source of economic growth and prosperity to Australia, it is also an **enabler of growth through digital transformation in every sector of the economy**. As businesses rely on the confidentiality and integrity of digital information, a strong domestic cyber security sector is critical for Australia's competitiveness and international reputation as a trusted place to do business, and for the nation's continued economic growth.

Australia is an ideal growth environment for cyber businesses

Australia's cyber security sector has a strong reputation internationally. Australia ranks as the world's seventh most committed cyber security country , according to the International Telecommunication Union's 2017 Global Cybersecurity Index.[1] Australia's 'cyber maturity' is the second highest in the Indo-Pacific, according to an annual survey by the Australian Strategic Policy Institute, which assesses how well governments worldwide invest in cyber security policies and legislative structures, business and digital economic strength, responses to financial cybercrime, military organisation, and social cyber awareness.[2] The Global Open Data Index also ranks Australia second in the world for policies that support cyber security and allow government data to be openly available to the public.[3]

Australia offers an ideal growth environment for cyber businesses, thanks to strengths in core research areas like quantum computation, wireless technology, trustworthy systems and niche high-value hardware. Further drawcards for investment include Australia's large services economy, quality education system, sound governance settings, economic stability, low sovereign risk and high living standards. The proximity to the fast-growing and increasingly digitised Indo-Pacific region adds to Australia's natural advantages.

These existing strengths put Australia in a favourable position to develop a vibrant and globally competitive cyber security sector. Economic analysis shows **the sector has the potential to almost triple in size in coming years**, with revenues soaring from just over A$2 billion in 2016 to A$6 billion by 2026.[4]

To seize the extensive opportunity, Australia needs to act urgently

Several hurdles are making it difficult for Australia to fully harness existing advantages and develop a sizeable world-class cyber security sector. To capitalise on the enormous opportunity in cyber, Australia must address its skills shortage, focus efforts in research and development, improve the environment for startups, enhance access to global markets, and robustly measure the growth of the sector and its impacts on the broader economy. The Australian economy needs to nurture a sophisticated and resilient cyber security culture. This requires a shift in mindset for decision makers within businesses as well as across the entire spectrum of employees, suppliers, and policymakers. More organisations will identify the value in investing in and supporting cyber capability when they recognise cyber security extending beyond risk mitigation and understand its role in driving economic growth.

1   International Telecommunication Union (2017). *Global Cybersecurity Index (GCI) 2017.* Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.
2   Australian Strategic Policy Institute (2017). *Cyber maturity in the Asia-Pacific Region 2017.* Available at: https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017.
3   Open knowledge international (2017). *Global Open Data Index – Australia.* Available at: https://index.okfn.org/place/au.
4   Australian Cyber Security Growth Network (2017). *Cyber Security Sector Competitiveness Plan.*

KEY FINDINGS

Tackling the cyber security skills shortage

New research, undertaken exclusively for this (2019) updated Sector Competitiveness Plan, draws on a range of job market data, showing that the skills shortage in Australia's cyber security sector is more severe than initially estimated and is already producing real economic costs.

Australia may need **almost 17,000 additional cyber security workers by 2026** for the sector to harness its full growth potential. The workforce shortfall has significant economic consequences. In 2017, the domestic cyber security sector is estimated to have forfeited up to $405 million in revenue, which companies could have generated if they had been able to find enough cyber security workers to fill existing vacancies.

The good news is **education providers have sprung into action** over the past year to cater for the growing demand for cyber security talent in Australia. Approximately half of all universities in Australia are now offering cyber security as a specific degree or as a major in IT or computer science degrees. The vocational education and training sector is increasing its emphasis on cyber security education. Leading TAFEs around the country joined forces in late 2017, coordinated by AustCyber, to play a greater role in providing nationally consistent cyber security training.

Together, these new cyber-specific degrees, certificates and diploma level courses will have a strong positive impact on Australia's future cyber security workforce. It is expected that **the number of cyber graduates could quadruple** from around 500 per year in 2017 to about 2,000 a year in 2026, based on the current course offerings by cyber security education providers.

However, this still leaves a significant shortfall of workers in the medium-term. Analysis for this Sector Competitiveness Plan shows there are risks to this mobilisation in the education system, and **more action is required**.

Australia needs to nurture early interest in cyber security to attract the best and brightest to the sector, continue to ramp up cyber security education and training, create industry-led professional development pathways. We also need to help workers with related skills transition from the wider IT sector and other industries into the diverse range of cyber security technical and non-technical work roles required by employers.

Overcoming the research and development challenge

Australia continues to demonstrate excellent and world-leading cyber security research capability. However, there are signs that its system of research and commercialisation is less efficient than in other leading cyber security nations such as the US and Israel.

Scattered public funding for cyber security research and development weakens Australia's ability to lead on innovation. Limited collaboration between the research community and the private sector further undermines the commercialisation of basic research ideas into marketable solutions.

In 2017 the Australian Government acknowledged that cyber security is a strategic priority and invested $50 million over seven years into **a new industry-led Cyber Security Collaborative Research Centre (Cyber Security CRC)** which commenced operation in mid-2018. The government funding adds to almost $90 million from a consortium of 25 industry, research and government partners, and will be critical to strengthening Australia's cyber security research and development capabilities.

The Australian Research Council has also incorporated cyber security into its funding priorities for the Industrial Transformation Research Program. The scheme is intended to fund research hubs and research training centres. It also helps students in Higher Degree by Research and postdoctoral programs to gain practical skills and experience through placement in industry.

AustCyber's Projects Fund provides a further $15 million over three years to finance industry-led projects aligned to the Knowledge Priorities outlined in this document, along with ten Sector Challenges supporting sustained sectoral growth. It encourages businesses to collaborate with academics to seed ecosystem-wide outcomes.

Australia needs to continue to improve research focus and collaboration to assist commercialisation – replacing the scattered approach to public research and development funding with a more targeted strategy that plays to Australia's strengths – and make access to seed and early-stage venture capital easier.

Removing market barriers for small Australian cyber security companies

Australia is home to a growing number of globally successful cyber security companies. These companies have proven their ability to develop and commercialise innovative cyber security products and services. Yet many others, particularly startups, continue to face barriers to growth. They often lack the business acumen, established credibility and scale to win key contracts with large industry or government customers in Australia and abroad.

In 2017, AustCyber launched a new platform called GovPitch where small businesses can present innovative cyber security ideas directly to public sector officials. The initiative is designed to **help startups gain anchor customers and grow quickly** by providing an alternative procurement pathway.

To better connect small businesses to the Chief Information Security Officers (CISOs) of ASX-listed companies, AustCyber and CISO Lens partnered on a new program called *Sky's the Limit*.

> Australia needs to continue efforts to help startups find their first customers, including analysing barriers and risks to government agencies and established businesses working with startups, promoting partnerships, providing coaching, showcasing Australian cyber security products and services to potential customers, and simplifying procurement processes.

Measuring the growth and development of the Australian cyber security sector and its impacts across the economy

New analysis for the 2019 update

Because cyber security as an industry is relatively new, Australia's standard classifications of industries and occupations do not accurately capture the sector's activity well. Cyber security as a business activity, as well as economic endeavour, cuts across multiple sectors and industries including critical infrastructure, services and technologies. It includes not only cyber security providers who comprise the cyber security sector, but also organisations in other sectors that employ cyber security specialists and skilled personnel. Further, cyber security products and services protect and enable much of the digital economy, but the benefits of cyber security have not been studied to the necessary depth and richness.

Solving these measurement challenges will allow governments to form more robust and sophisticated industry development policies; encourage investment in the sector as well as into building organisational cyber security resilience; and help cyber security companies to understand their commercial surroundings and the growth opportunities available to them.

> Australia needs to improve measurement of the Australian cyber security sector and its impact to enhance understanding of the sector and track progress on addressing other sector challenges. Measurement of fundamental economic metrics such as the size of the sector and its value add to the economy can serve as a foundation for analysis of the broader impacts of cyber across the economy, including its role as an enabler of growth and its contribution to overall prosperity.

An action plan to position Australia as a world-leading cyber security nation

The Sector Competitiveness Plan sets out strategies and actions that Australian governments, the private sector, training and research institutions, and AustCyber can undertake to ignite growth in Australia's cyber security sector. Figure 1 provides an overview of the key elements of the Sector Competitiveness Plan.

Figure 1

Challenges

Research and commercialisation
Lack of research focus, weak collaboration and difficulties accessing capital are constraining strong basic research

Firm growth and export
Credibility gaps and market barriers make it hard for firms to grow in Australia, while service models hamper export growth

Skills and workforce
Lack of job-ready cyber professionals and under-developed transition pathways have led to skills shortages

Measurement
Lack of robust measurements about the sector means there is an information vacuum, leading to uncertainty

Key goals / Strategies

1 Grow an Australian cyber security ecosystem
- Help cyber security startups find their first customers
- Improve research focus and collaboration to assist commercialisation
- Make access to seed and early-stage venture capital easier
- Simplify government and private sector procurement processes
- Provide robust measurement of the ecosystem's development and impact on the Australian economy

2 Export Australia's cyber security to the world
- Support Australian firms to develop scalable service delivery models
- Develop cyber security as an educational export
- Attract multinational corporations to use Australia as an export base for the region

3 Make Australia the leading centre for cyber education
- Attract and retain the best and brightest to cyber security
- Create vibrant, industry-led professional development pathways
- Ramp up cyber security education and training

1 THE GLOBAL OUTLOOK FOR CYBER SECURITY

"

Disruptive technological trends will continue to evolve and, as a result, generate demand for new cyber security solutions

1.1 OVERVIEW

The world is abuzz with new connections. Cars, fridges, houses, factories – the list of things that can be controlled and monitored remotely grows daily. At the same time, more and more people around the globe have access to these new technologies and depend on them in their daily life. But the mass of interconnected things, referred to as the Internet of Things (or Internet or Everything), and technological innovation comes with a risk: it increases the number of potential targets for malicious cyber activity.

Malicious cyber activity is a growing challenge for organisations worldwide. It ranges from straightforward online fraud – such as scams using email, websites or chat rooms – to sophisticated cyber espionage and calculated cybercrime, used to steal secrets and other information stored digitally on systems and networks. Malicious cyber activities have the potential to seriously harm not just an organisation's business and reputation, but also to compromise a nation's security, stability and prosperity. The number of incidents has spiked in recent years, as perpetrators aggressively exploit flaws in digital infrastructure. This has catapulted cyber security to front-of-mind for business leaders, regulators and politicians who are anxious to shore up defences and improve resilience.

Cyber adversaries are constantly devising new ways to exploit vulnerable systems and networks. This is forcing organisations – from banks to energy companies, and from government agencies to charities – to strengthen their cyber defences. The growing security needs of organisations are expected to underpin the rapid evolution of the global cyber security sector, which provides a substantial opportunity for cyber security businesses in Australia.

Over the next decade, the industry will become more diverse and sophisticated, as businesses continue to refine their product offerings to meet their customers' varying cyber security needs. However, the outlook for security needs and the main product types (hardware, software and services) is not uniform. It is driven by differences in current size, projected demand, export potential and ability to create more jobs.

The Internet of Things, Cloud Computing and the convergence of IT and operational technology (OT), are some of the current important disruptive technological trends that will contribute to the future demand of cyber security solutions. They will increase demand for all forms of cyber security, particularly software. These disruptive technological trends will continue to evolve and, as a result, generate new demand for new cyber security solutions.

1 THE GLOBAL OUTLOOK FOR CYBER SECURITY

1.2 CYBER SECURITY SPENDING IS GROWING FAST

Demand outlook

Spending on cyber security worldwide is expected to soar over the next decade. The global cyber security market is currently worth around US$145 billion and is set to increase by 86 per cent to US$248 billion by 2026, as shown in Figure 2. Roughly three-quarters of the global expenditure on cyber security comes from cyber security 'users' (organisations and individuals seeking to defend themselves against malicious cyber activity) purchasing the products and services of external cyber security 'providers' (both specialist cyber security companies and IT or telecommunications companies with cyber security offerings). The remaining quarter of spending covers all internal expenditure on cyber security, mainly the cost of employing in-house teams with specialist cyber security skills.[5]

The global cyber security market is currently worth around US$145 billion and is set to increase by 86 per cent by 2026

Analysis based on available market data and expert interviews suggests this trend will accelerate in the future. While money spent on in-house or internal cyber security functions is expected to grow by around 7.2 per cent each year to 2026, global spending on external cyber security products and services is set to increase by 8.4 per cent annually over the same period.

The global cyber security market is currently worth around US$145 billion and is set to **increase by 86 per cent** by 2026

---
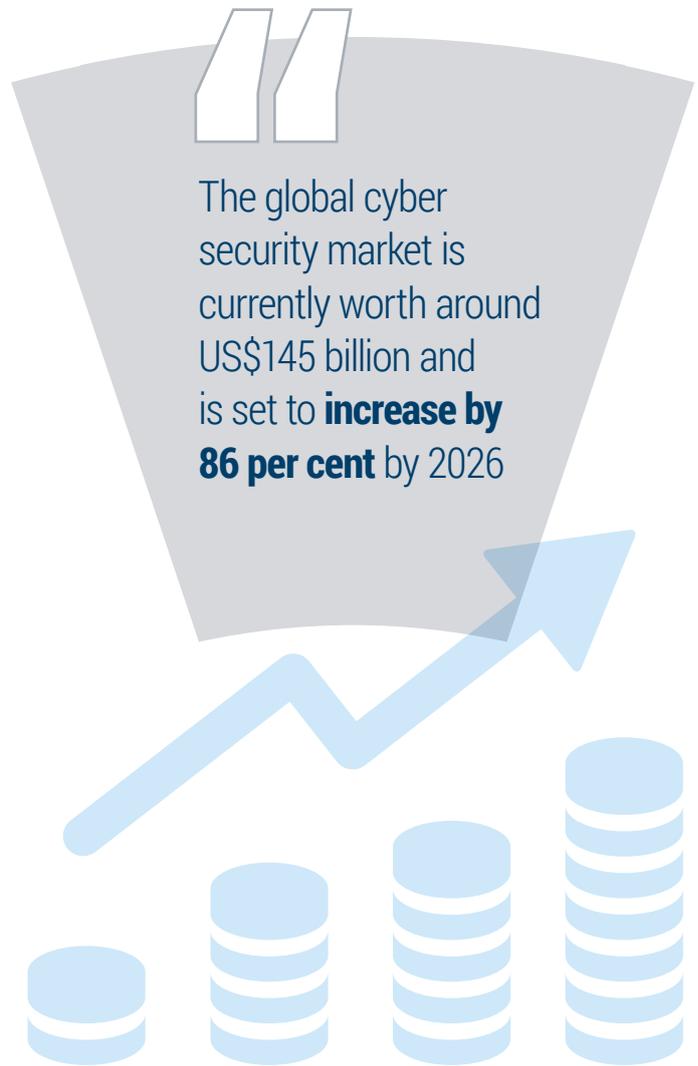
5   Internal expenditure on cyber security is more difficult to measure than external spending, as enterprises are often wary of disclosing their investment in internal cyber capabilities due to security concerns. While this plan focuses primarily on external spending, it proposes several actions (including skills development) that would strengthen both outsourced cyber providers and in-house cyber security teams.

Figure 2

Global cyber security spend

US$b per annum, 2018 = latest actual data* (constant exchange rates)

Legend: External† (light blue), Internal§ (dark blue)

+125B (+86%)

270

Compound annual growth rate (CAGR) 2018–2026

Year	External	Internal	Total
2012	63	25	88
2013	68	26	95
2014	74	27	101
2015	84	29	113
2016	92	31	122
2017	99	32	131
2018	109	36	145
2019	119	39	159
2020	130	42	173
2021	141	46	187
2022	153	49	202
2023	164	52	216
2024	178	55	233
2025	192	59	251
2026	207	62	270

External CAGR: 8.4%

Internal CAGR: 7.2%
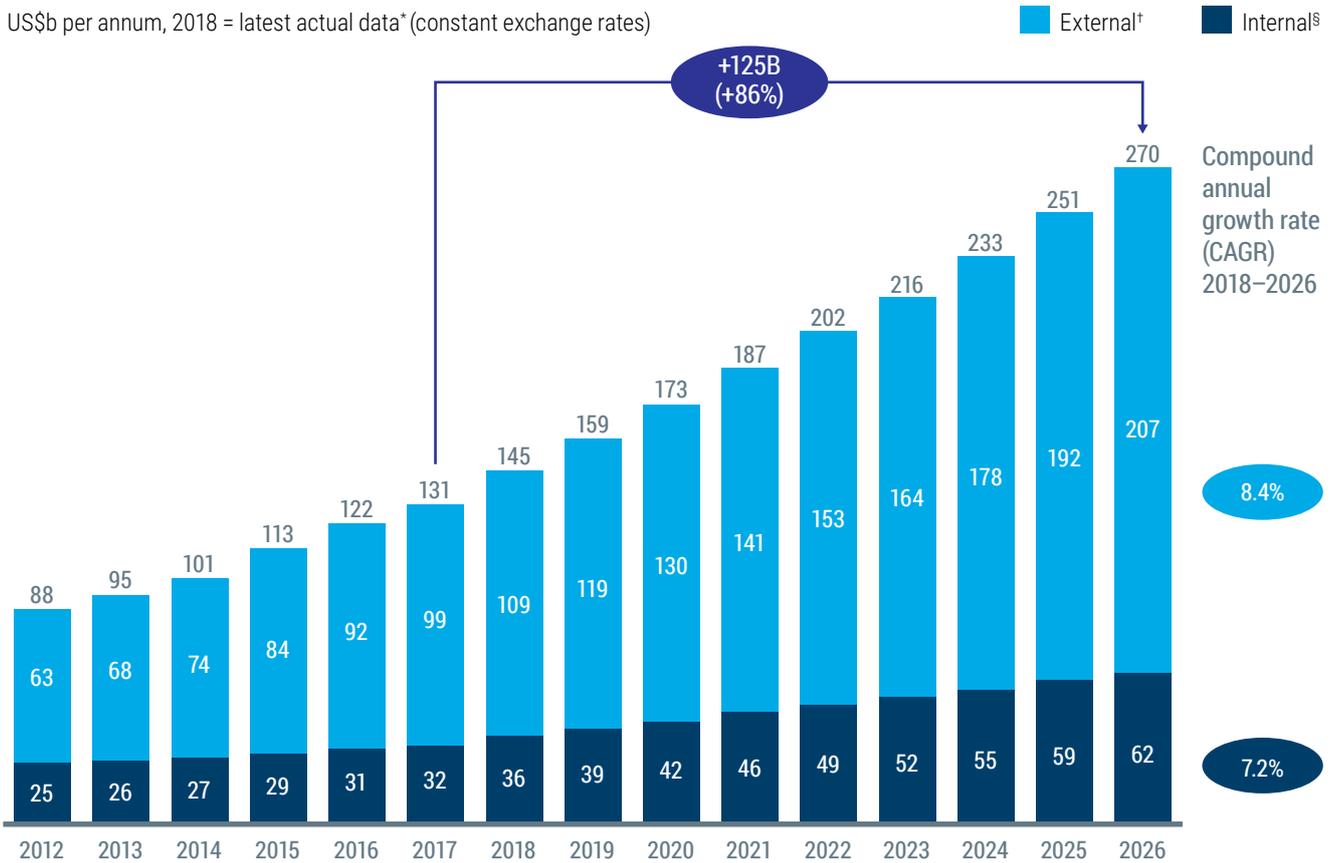
* 2012–2016 data based on Gartner data as at 3Q16; 2017 and beyond based on Gartner data

† External spend based on forecasts to 2023 provided by Gartner, extrapolated to 2026 using the average growth rates. Growth rates applied at the product segment level

§ Internal spend refers to the compensation of in-house full-time equivalent employees. Estimated based on Gartner data on global internal spending. Internal spend grows more slowly than external spend, linked to the increasing adoption of external managed security services

SOURCE: Gartner; Australian Bureau of Statistics; Burning Glass; expert interviews; AlphaBeta and McKinsey analysis

1 THE GLOBAL OUTLOOK FOR CYBER SECURITY

The demand outlook for Australia's neighbours is particularly strong (see Figure 3). Cyber security spending in the Indo-Pacific region, which includes Asia Pacific nations as well as China and India, is expected to increase faster than the global average, with an additional US$40 billion in spend by 2026. This means Indo-Pacific countries have emerged as significant buyers of cyber security solutions, set to account for roughly one-quarter of global cyber security spending in 2026. The fast-rising demand from countries in Australia's vicinity adds to the market opportunity for Australian cyber security providers.

> "
> Indo-Pacific countries have emerged as significant buyers of cyber security solutions, adding to the market opportunity for Australian providers

Figure 3

Indo-Pacific (Asia-Pacific including China and India) cyber security spend

US$b per annum, 2018 = latest actual data* (constant exchange rates)   External†   Internal§
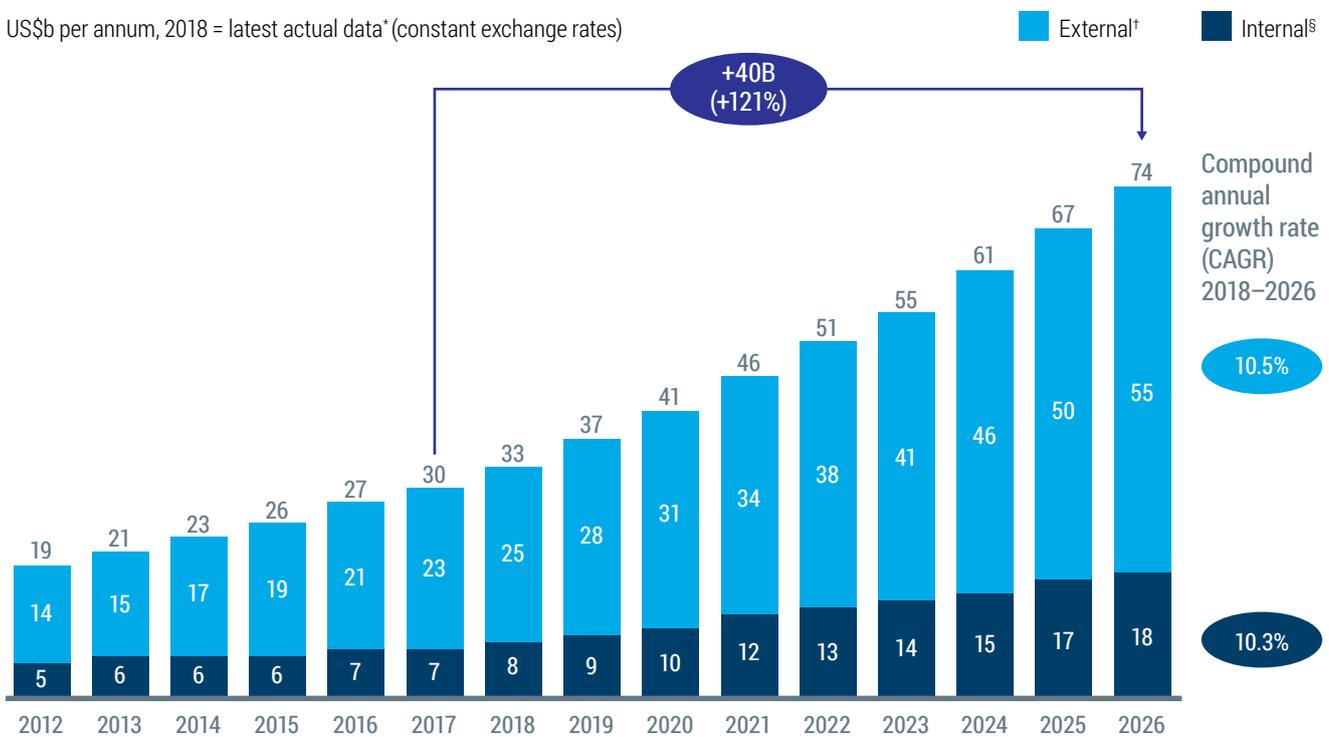
* 2012–2016 data based on Gartner data as at 3Q16; 2017 and beyond based on Gartner data as at 4Q17
† External spend based on forecasts to 2023 provided by Gartner, extrapolated to 2026 using the average growth rates. Growth rates applied at the product segment level
§ Internal spend refers to the compensation of in-house full-time equivalent employees. Estimated based on Gartner data on global internal spending. Internal spend grows more slowly than external spend, linked to the increasing adoption of external managed security services

SOURCE: Gartner; Australian Bureau of Statistics; Burning Glass; expert interviews; AlphaBeta and McKinsey analysis

Demand drivers

Several trends support the growth outlook for cyber security spending:

- **Expanding threat of cyber attacks** – Malicious cyber activity is on the rise, as criminals use ever-more sophisticated strategies to infiltrate systems and networks. For example, there were over 11.7 billion records and over 11 terabytes of data leaked or stolen in publicly disclosed security incidents in the three years from 2016 to 2018, according to the technology company IBM.[6] Software provider Symantec Corporation discovered 670 million new unique pieces of malware in 2017 and just over 245 million in 2018. The frequency of so-called mega breaches, defined as the loss or theft of more than 10 million personal data records at once, has soared to record highs globally.[7] But official numbers are likely only the tip of the iceberg, as more and more companies choose not to reveal the full extent of the data breaches they experience. Cyber threats have increased markedly in Australia too. During 2016–17, malicious emails alone caused businesses in Australia to report losses of more than A\$20 million, an increase of over 230 per cent from the A\$8.6 million reported the previous financial year.[8] Again, this figure likely represents only a small percentage of total malicious cyber activity, due to both misreporting and underreporting.

- **Mounting exposure to cyber risk** – The rapid expansion of internet-enabled economic activity and the number of connected devices and systems increase the likelihood of widespread malicious cyber activity. People in far corners of the globe are gaining online access, as the world becomes more digitised and interconnected. This is partly due to smartphone penetration, which has risen markedly in many countries. Everyday items such as watches, fridges and cars are now internet connected, as are important customer databases, power plants and government payment systems. This increases the volume and quality of information shared electronically, and widens the range of potential targets for perpetrators.

- **Growing risk awareness** – Recent high-profile cases of malicious cyber activity and media coverage of data breaches have made companies and other organisations increasingly aware of the risks cyber adversaries pose to their businesses. Latest research from Telstra, Australia's largest telecommunications provider, shows that 78 per cent of organisations surveyed globally, including 76 per cent of Australian respondents, have an incident response plan in place.[9] As of February 2018, many businesses in Australia are now required to notify victims and the Privacy Commissioner of data breaches, which will drive further awareness and accountability. The growing awareness is increasingly driving companies to adopt frameworks including security audits, risk assessments, compliance tools and continuous end-user training.

- **Increasing regulation of cyber risk** – Governments worldwide are increasingly concerned that cyber attacks could hit crucial economic sectors. Many are issuing new laws to ensure organisations bolster their cyber security controls. The expected growth in cyber-related regulation is likely to prompt organisations to increase their security spending. For example, increasing regulatory oversight has already forced banks and insurance companies to be more acutely aware of malicious cyber activity threatening their operations. The new data breach notification laws in Australia now require all businesses with an annual turnover of \$3 million or more to publicly disclose any case where they believe personal data was compromised, or risk hefty fines. Similar laws have been in place in the US for years. In the EU, new data protection regulation, including privacy provisions, came into force in May 2018. Such mandatory standards will almost certainly lead to higher demand for new cyber security products and services – a recent survey shows that almost half of all Australian small and medium-sized businesses with an annual turnover of over \$3 million do not consider themselves prepared for the new disclosure laws.[10]

---

6   IBM Corp (2019). IBM X-Force Threat Intelligence Index. Available at: **https://www.ibm.com/security/data-breach/threat-intelligence**.

7   Symantec Corp (2019) Internet Security Threat Report. Available at: **https://www.symantec.com/security-center/threat-report**.

8   Australian Cyber Security Centre (2017), *Threat Report*. Available at: **https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf**.

9   Telstra (2019). Telstra Security Report. Available at: **https://www.telstra.com.au/business-enterprise/news-research/security/research/security-report-2019**.

10   HP (2018), *HP Australia IT Security Study*. Available at: **https://www.data3.com/wp-content/uploads/2018/02/Fact-Sheet-HP-Australia-IT-Security.pdf**.

1.3 THE CYBER SECURITY MARKET IS DIVERSE AND SOPHISTICATED

Cyber security is no longer just firewalls and off-the-shelf virus software. In recent years, it has evolved significantly to encompass a sophisticated range of products and services, as well as activities within organisations to build and operate their cyber security system.[11] Cyber security today is best defined and understood as the collection of tools, technologies, processes and practices that can be used to protect networks, computers and data from unauthorised access or attack. This broad definition, based on the definition used by the International Telecommunications Union, captures the multidisciplinary nature of cyber security practice today.[12]

Figure 4

Examples of product types and security needs

		Security need		
		1 Protection stack		
		Core system protection and management	**Application protection**	**Protection of endpoints and data at rest**
Description of security need		• **Prevent attackers** from **gaining access** to a company's network and infrastructure	• **Protect 3rd party and custom applications** and systems performing critical tasks within the network	• Provide **advanced differential protection of core assets** inside the core system
Product types	**Hardware**	• Secure mobility devices • Next generation firewalls • Router switch control • Virtualised environment for malware detonation • Sandbox	• n/a	• n/a
	Software	• Intrusion prevention system (IPS) • Anti-DDoS protection • Malware protection • Unified threat management • Automated vulnerability scanning • Private cloud security	• Automated application code scanning • Secure messaging (antispam, antimalware, secure email, content filtering) • Secure web (filtering)	• Antivirus (AV)/antimalware • Data loss protection (DLP) • Digital rights management (DRM) • Mobile device management (MDM) • Encryption
	Services	• Firewall configuration and management • Threat intelligence and signature feeds • Penetration testing • Malware identification	• Application patch management • Application testing/code review • Software Development Life Cycle (SDLC)	• Patch and configuration management • Endpoints/ Hardware • Network

11 This Sector Competitiveness Plan mainly focuses on the delivery of cyber security products and services to organisations. While individuals do purchase cyber security products, they account for less than 6 per cent of global demand. Gartner (2016), *Information Security, Worldwide, 2014–2020, 3Q16 Update.*

12 International Telecommunications Union (2018), 'Definition of cybersecurity'. Available at: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

*Cyber security is no longer
just firewalls and off-the-shelf
virus software*

Three fundamental security needs shape demand for cyber security products and services: the 'protection stack'; security operations; and underlying processes. Matching the different security needs and product types, as shown in Figure 4, provides a helpful structure for understanding the diversity of the global cyber security sector.

2 Security operations			3 Underlying processes	
Security management, assessments, and analytics	**Incident recovery and response**	**Identity and access management**	**Governance, risk and compliance**	**Awareness, training, and oversight**
• Assess current risk, maturity, and **vulnerabilities** and **manage** a full spectrum of **security operations**	• **Respond to an incident** by identifying, investigating and remediating vulnerabilities and restoring service	• Provide **tools and governance model/ processes** to control access to information	• **Align IT security with enterprise risk** and ensure continued compliance	• Create a more **IT secure culture** and **reduce risk** of human-centered vulnerability
• n/a	• Intrusion detection system (IDS), as hardware • Secure mobility devices	• 2FA hardware (e.g. tokens)	• n/a	• n/a
• Security information and event management (SIEM), incl. Level 1 response • Log management	• Intrusion detection system (IDS), as software • Automated malware detection • Data discovery	• Identity management • Active directory integration • Privileged user tracking • LDAP and single sign-on • Network access control (NAC)	• Governance/ compliance tracking • Risk reporting	• Automated security reporting • Learning modules
• Level 2/3/4 SIEM response (outsourced SOC) • Log analytics	• Incident response (CIRT) • Incident investigation and post-mortem • Forensics and malware analysis • Incident recovery	• User provisioning/ deprovisioning • Access rights/ entitlement management	• Strategy development • Risk and vulnerability assessments	• Technical IT security training • Employee training • User training

1 THE GLOBAL OUTLOOK FOR CYBER SECURITY

Security needs

Three security needs drive demand for cyber security products and services:

- **Building a 'protection stack'** – This is the basic infrastructure that protects an organisation's IT networks and computer systems. It includes basic hardware, such as firewalls, routers and sandboxes, and a range of software tools including intrusion prevention systems (IPS). Organisations also need to protect software applications and systems that perform critical network tasks, and they need to ensure the endpoints of their network (such as user devices) are properly managed and secured.

- **Maintaining operational security** – Once they have established a basic security infrastructure, organisations need to monitor and maintain their safety networks and systems. Some maintenance tasks are fundamental and ongoing, for example the security assessment and associated analytics to identify risks and detect attacks on their networks. Organisations also need to maintain their identification and access management systems to ensure only authorised staff enter their networks. When cyber security incidents do occur, organisations must have the capability to respond to the incident, fix weaknesses and restore their systems.

- **Strengthening underlying structures** – To successfully fend off cyber adversaries, an organisation must create a strong culture of risk awareness. This includes clear rules for compliance, governance and risk management and ensuring all staff are well-trained and conscious of common cyber security threats.

Security needs of vary depending on an organisation's size and the sector it operates in. Security needs also evolve over time depending on the maturity of an organisation's cyber security strategies, changes in technology and the shifting nature of cyber threats. Most organisations meet these needs through a combination of internal capabilities and external cyber security providers.

Product types

An organisation can meet its cyber security needs through a combination of hardware, software and services. All three product types are embedded in distinct markets that vary in size and growth rate, exportability, potential for job creation and job quality (wage level and security of jobs). Technological trends also affect these three product types differently.

Dividing the cyber security sector into these three basic product types remains meaningful and useful for this analysis, even with some areas of overlap between product types. For example, software is increasingly delivered as a service rather than a standalone product, and hardware devices are often combined with proprietary software.

Hardware

Hardware manufacturers build the physical devices, such as firewalls and encrypted USB flash drives, that help protect IT networks against malicious cyber activity.

- **Size** – Hardware forms the smallest product type of the cyber security sector, accounting for roughly 10 per cent or US$10.6 billion, of external cyber security spending globally in 2018. It is most heavily concentrated in the protection stack, with the bulk of revenue generated by providing clients with core system protection and management. Outside the protection stack, spending on hardware is very limited (see Figure 5).

- **Growth** – While the global demand for cyber security is projected to increase significantly over the next decade, hardware producers will receive a relatively small though focused share of the sector's growth. The external global spending on physical IT protection equipment is estimated to increase by US$6.9 billion by 2026, equivalent to an average growth rate of 6.5 per cent per year. This represents only a fraction of the projected total industry external demand growth of more than US$98 billion over the same period.

- **Exportability** – Cyber security hardware manufacturers have ample scope to export their products and compete in a global marketplace with relatively few barriers. The Wassenaar Arrangement may limit exports of some cyber security hardware products with potential use in defence. The Wassenaar Arrangement is a multilateral export control regime covering 41 states including Australia.[13] It promotes transparency and information exchange to ensure the transfer of certain goods and technologies, particularly those with dual-use, does not enhance military capabilities that would undermine international and regional security and stability.

- **Job creation and quality** – Hardware production supports an average of 4.6 full-time jobs per US$1 million of annual revenue generated, a labour intensity that ranks between software and services (see Figure 6). The quality of jobs in hardware varies widely from design (with high-skilled, high-wage jobs that are unlikely to be automated) to manufacturing (with lower skills required and higher susceptibility to automation).

13   Full title: Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

Figure 5

Breakdown of global cyber security spend

Billions US$, 2018

Larger ▰▰▰▱▱ Smaller

Security need

Product type*	1 Protection stack	2 Security operations	3 Underlying processes	Total
Hardware	$8.7 B	$1.9 B	N/A	$10.6 B
Software	$20.7 B	$9.6 B	$3.2 B	$33.5 B
Services	$24.6 B	$29.2 B	$11.1 B	$65.0 B
Total	$54.0 B	$40.7 B	$14.3 B	$109.1 B

Global spend on services is significantly larger than both hardware and software together
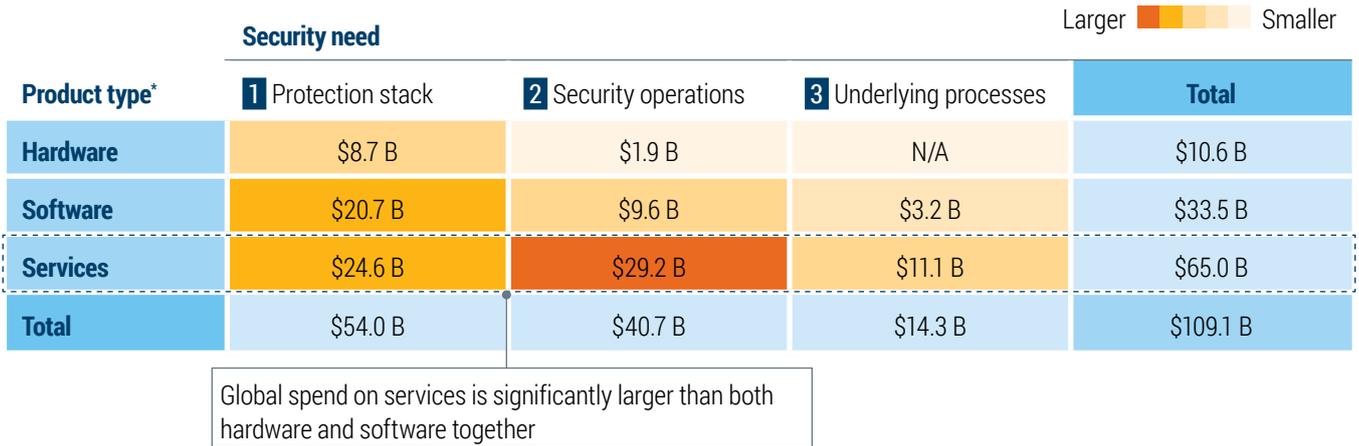
Note: Cells may not sum to totals due to rounding, estimates only

* Hardware refers to physical devices (e.g. firewalls); services includes consulting, MSS, implementation and support services

SOURCE: Gartner; IDC; expert interviews; AlphaBeta and McKinsey analysis

Figure 6

Job intensity

Job intensity by segment*

FTEs per $1M USD of annual revenue, estimates only

The services segment supports around 6.4 jobs per $1M USD of revenue (equivalent to a revenue per job of $156,000)

Hardware: 4.6
Software: 4.0
Services: 6.4

Industries used as proxies

Hardware	Software	Services
Average of: • Computer system design • Equipment manufacturing	Average of: • Computer system design • Internet services	Weighted† combination of: • Data processing services • Professional services • Administrative services

Job intensity by type of service

FTEs per $1M USD of annual revenue

High-skill technical (e.g. forensics): 3.1
High-skill non-technical (e.g. risk consulting): 9.1
Low-skill (e.g. IAM): 13.4
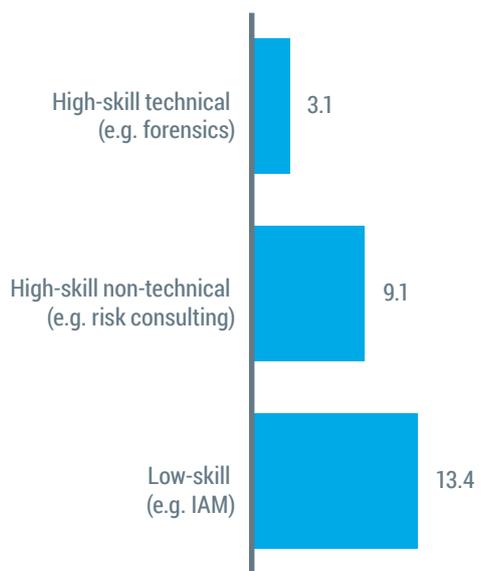
* Estimated based on revenue per worker data for similar industries in Australia. Estimates for 2016

† Weights based on distribution of spend across security needs, combined with a judgment of the most appropriate proxy for each security need

SOURCE: Australian Bureau of Statistics, Gartner, AlphaBeta and McKinsey analysis

Software

Software companies within the cyber security sector create the applications that help organisations defend their computer systems and IT networks against intrusion and unauthorised use. Typical examples are applications for secure messaging, anti-malware, anti-spyware, identity management and network access control.

- **Size** – Software represents the cyber security sector's second-biggest product type. In 2018, it accounted for more than US$33 billion of the world's total external cyber security spending, or around 30 per cent of the sector's revenue, as shown in Figure 5. The use of software is currently concentrated around the protection stack, providing application protection, protection of endpoints and data at rest, and offering programs for the core system protection and management. It is also used in operational security, particularly for identity and access management.

- **Growth** – The growth outlook for cyber security software is strong. In the seven years to 2026, external demand for cyber security software is expected to increase at an average annual rate of 9.5 per cent. This demand growth is forecast to be strongest in security operations, as users seek more effective solutions for security assessment and analytics, and identity and access management. Application protection, currently the largest security need in software, is expected to remain an area of focus.

- **Exportability** – The market for cyber security software is strongly globalised, with relatively few barriers to trade. This has led to a concentration of market share in a small number of countries: companies domiciled in the US control 61 per cent of the global market, while Israeli companies dominate around 18 per cent.[14] However, country-specific rules protecting intellectual property could act as a barrier to export software.

- **Job creation and quality** – Figure 6 shows cyber security software tends to be less labour intensive than cyber security hardware or services, supporting an average of 4.0 full-time jobs per US$1 million of annual revenue. Cyber security software jobs are typically of very high quality and hard to automate, requiring high-skilled and well-paid staff.

Services

Cyber security service providers meet a broad range of security needs for organisations. For example, they may help manage an organisation's core computer system defences, assess network vulnerabilities or provide a security strategy plan. Some act as 'first responders' when an organisation has a security incident, while others offer specialised advice on risk and compliance issues.

- **Size** – Services form the largest product type in the cyber security market, generating around 60 per cent, or US$65 billion, of the sector's global external revenue, as shown in Figure 5. Demand is highest in security operations, and specifically in security management, assessment and analytics (a sub-segment of security operations). This includes, for example, setting up real-time monitoring systems for servers, endpoints and network traffic to rapidly detect any potential malware or data loss. Companies in the security operations segment attract almost 45 per cent, or US$29 billion, of the entire global spending on external cyber security services.

- **Growth** – Services enjoy the strongest growth outlook within the global industry. From 2018 to 2026, the global spending on external cyber security services is expected to increase by 8.1 per cent per year. Growth is expected to be strongest for security operations, with an additional US$56 billion in demand forecast over the period to 2026.

- **Exportability** – Cyber security services are exportable, but country-specific regulation and IT infrastructure can make the services trade more challenging. For example, companies that help configure and manage their client's firewall may be limited in their reach by existing cross-border data regulations. Similarly, companies offering security management, assessment and analytics worldwide may require local offices to effectively service customers abroad. The assessment in Figure 7 shows that such factors affect exportability of incident recovery and response services the most, while application protection services and awareness, training and oversight are the least affected.

---

14   International Data Corporation (2016), Worldwide Security Spending Guide 1H 2016 Update.

- **Job creation and quality** – Figure 6 shows that, on average, services support 6.4 full-time jobs per US$1 million of annual revenue, marking the highest rate of job creation among the three product types. However, the quality of services jobs is less consistent and tends to be lower than cyber security jobs in the hardware and software segments of the industry. Services jobs in identity and access management, for example, typically require lower skills and pay lower wages than others. Automation is also more likely to impact services than other areas of cyber security, as advanced machine learning and artificial-intelligence (AI) software will continue to take over an increasing number of tasks. This trend is particularly acute in relation to monitoring threats.

Figure 7

Assessment of the exportability of services to address different security needs

■ Limiting factor   ■ Partial limitation   ■ Not a limiting factor

Security needs		Specific examples	Example global players	Exportability			Overall exportability
				Subject to cross-border data regulations	Need for in-country core technical team	Need for in-country infrastructure	
1 **Protection stack**	Core system protection and management	• Firewall configuration and management • Threat intelligence and signature feeds • Penetration testing • Malware identification	• FireEye • iSight Partners	Partial limitation	Not a limiting factor	Limiting factor	Medium
	Application protection	• Application patch management • Application testing/ code review • SDLC	• Veracode • Lumension	Not a limiting factor	Not a limiting factor	Not a limiting factor	High

	Protection of endpoints and data at rest	• Patch and configuration management
		  - Endpoints/Hardware
		  - Network
			• Qualys
			• Secunia
				Partial limitation	Not a limiting factor	Partial limitation	Medium

2 **Security operations**	Security mgmt, assessments, and analytics	• Level 2/3/4 SIEM response (outsourced SOC) • Log analytics	• Symantec • IBM	Limiting factor	Not a limiting factor	Limiting factor	Medium (high for the low-end component)
	Incident recovery and response	• Incident response (CIRT) • Incident investigation and post-mortem • Forensics and malware analysis • Incident recovery	• FireEye • Kroll	Partial limitation	Limiting factor	Limiting factor	Low
	Identity and access management	• User provisioning/ deprovisioning • Access rights/ entitlement management	• Okta • Covisint	Limiting factor	Not a limiting factor	Not a limiting factor	Medium
3 **Underlying processes**	Governance, risk and compliance	• Strategy development • Risk and vulnerability assessments	• Deloitte • KPMG	Not a limiting factor	Partial limitation	Not a limiting factor	Medium
	Awareness, training, and oversight	• Technical IT security training • Employee training • User training	• SANS • Infosec	Not a limiting factor	Not a limiting factor	Not a limiting factor	High

SOURCE: Expert and stakeholder interviews; AlphaBeta and McKinsey analysis

1.4 TECHNOLOGY IS RESHAPING THE INDUSTRY

While technological change affects every industry, the cyber security sector is affected more than most. Several major trends are likely to unfold in coming years, which will shape the structure of cyber security markets. For some organisations, many of the looming technological changes will be disruptive. For others, they could work as a tailwind.

Analysis suggests that software companies generally appear best positioned to benefit from the following five major technological trends:

• **Convergence of information technology and operational technology** – Historically, technologies used to control production plants and machines (operational technology, or OT) have differed from computer hardware and software technologies used to manage the an organisation's general data flow. Over the last few years, however, operational technologies, such as sensors to monitor the temperature or water pressure during production, have become increasingly computerised. More and more companies are now equipping their machine-monitoring devices with IT-like features to integrate computer systems, save cost and speed up production. This convergence of OT and IT leads to increasingly complex networks, with multiplying endpoints and data types requiring more sophisticated cyber defences. The vulnerability of these merged systems generates fresh demand for most security product types.

> The rapid increase in smart device usage worldwide is multiplying the number of endpoints in networks and propelling demand for cyber security products

• **Mobile internet** – The number of people who own a smart device and use the internet continues to climb. A survey by US research organisation Pew Research Center found that, across 11 industrialised countries, a median of 68 per cent of adults owned a smart device in 2015, with even higher rates of smart device ownership in Australia (77 per cent) and South Korea (88 per cent).[15] Smart devices are also on the rise in emerging and developing countries, where their penetration rate increased to 54 per cent in 2015, from 45 per cent two years earlier. Two thirds of adults worldwide use the internet, according to the research, and a growing share of them now use their mobile phones to go online. This rapid increase in smart device usage worldwide is multiplying the number of endpoints in networks and propelling demand for cyber security products. It is especially likely to drive investment in identity and access management.

---

15 Pew Research Center (2016), *Global Technology Report*, Available at: http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies.

- **Artificial intelligence and big data** – Rapid improvements in artificial intelligence and advanced machine learning are changing the modern workplace. Increasingly, computers are used to perform tasks that rely on complex analyses, subtle judgments, and creative problem solving – a trend coined 'automation of knowledge work'. McKinsey estimates that today's available technologies could automate 45 per cent of activities that people are currently paid to perform.[16] In cyber security, these advances are already starting to change the way threats can be identified, by reducing reliance on human network monitoring activities. This will benefit software developers, as companies increase their demand for applications to identify, analyse and manage cyber security threats. In the medium to long-term, service providers will be disadvantaged. However, the transition to greater automation will likely increase the demand for services in the short-term as cyber service providers support their customers to transition to more automated security systems.

- **Cloud computing** – The evolution of cloud computing technologies is becoming a major driver of business efficiency. The ability to store huge amounts of data and bundle an array of IT solutions in one location is a powerful tool for companies to save costs and simplify their IT infrastructure. Increased use of cloud technology has moved the potential area of malicious cyber activity from the corporate network to cloud infrastructure managed by third parties. This is prompting companies to think differently about how to secure their operations. Several cloud computing providers are already offering network protection products and services through the cloud itself. This reduces the need for companies to purchase their own cyber security infrastructure, dampening the outlook for hardware producers but generating more demand for security operations to manage and monitor access to the cloud.

- **Internet of Things** – The world of consumer products is turning into a network of interconnected things. Cars, buildings, fridges and countless other everyday devices are increasingly equipped with sensors, voice-control systems, internet access and data-processing features. Today, a smartphone can communicate with wearable devices to monitor a person's health, while smart cars can sync with a user's calendar to monitor petrol needs or plan routes. The growing number of interconnected devices, and the expansion in data types and volume, will increase the risks of malicious cyber activity. In turn this will generate new opportunities for providers of cyber security solutions. Software developers will particularly benefit, as new types of endpoints need to be secured.

Figure 8 summarises how these five major technological trends may impact the cyber security sector and its products.

Several other important technologies could also have profound implications for the structure of the cyber security sector. Two that are currently attracting attention are blockchain and quantum computing.

Quantum computing is considered a breakthrough technology still in development but that would spark a major upheaval in the current cyber security sector if it becomes a reality. Australian researchers are among the leaders in a global race to develop quantum computers, and home-grown startups like QuintessenceLabs are at the forefront of offering new quantum-safe encryption technologies (see Box 14).

Similarly, the disruptive power of blockchain technologies (digital ledgers of bitcoin or other cryptocurrency transactions) may bode well for Australia's well-established financial services industry.

It is difficult to predict how these trends will end up impacting different segments of the cyber security sector, but the potential for Australia to seize a competitive edge in both blockchain technologies and quantum computing is significant.

Any analysis of potentially disruptive technological trends needs to factor in a high degree of uncertainty, but this uncertainty is particularly stark in cyber security. Unlike other industries in the broader ICT sector, cyber security evolves around the existence of an adversary: it has to constantly respond to highly unpredictable, destructive activities. Despite best predictions and preparations, it is not possible to know exactly where future attacks will come from and how the sector will reshape in response.

---

16   McKinsey Quarterly (July 2016). Available at: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/where-machines-could-replace-humans-and-where-they-cant-yet.

1 THE GLOBAL OUTLOOK FOR CYBER SECURITY

Figure 8

Potential impact of technological trends on the cyber security sector

■ Positive effect   ■ No clear effect   ■ Limiting factor

Trend		Hardware	Protection stack		Security operations		Underlying processes	
			SW	Serv.	SW	Serv.	SW	Serv.
Convergence of IT and O`T	Information technology is converging with operational technology, increasing the complexity of technology systems and the vulnerability of operational systems	**Greater connectivity of operational tech will generate new demand across cyber needs and product types**						
		■ Positive	■ Positive	■ Positive	■ Positive	■ Positive	■ No clear	■ Positive
Mobile Internet	The rapid increase in smartphone penetration has increased the number of people worldwide who are connected and multiplied the number of endpoints in networks	**Multiplication of endpoints will drive investment in protection and identity and access management**						
		■ No clear	■ Positive	■ No clear	■ Positive	■ Positive	■ No clear	■ No clear
AI and big data	Rapid improvements in artificial intelligence and advanced machine learning are changing the way threats are identified	**Although automation of security testing and management will favour software, it will increase overall demand**						
		■ No clear	■ Positive	◨ Positive/Limiting	■ Positive	◨ Positive/Limiting	■ No clear	■ Limiting
Cloud	Cloud delivery of IT services is becoming increasingly dominant, with cyber security generally offered by the cloud provider	**Shift to cloud reduces companies' need for their own infrastructure and emphasises software and cloud**						
		■ Limiting	■ No clear	■ No clear	■ Positive	■ Positive	■ No clear	■ Positive
Internet of Things	Interconnection of increasing numbers of physical devices grows the number of endpoints and the types of data accessible	**Securing new endpoints and managing new types of threats made possible by IoT will be sources of growth**						
		■ Positive	■ Positive	■ No clear	■ Positive	■ No clear	■ No clear	■ No clear

SOURCE: Expert and stakeholder interviews; AlphaBeta and McKinsey analysis

28   AUSTRALIA'S CYBER SECURITY SECTOR COMPETITIVENESS PLAN: 2019 UPDATE

Box 1

Boomerangs: Australian-born successes expanding back home

Bugcrowd, Dtex Systems and UpGuard are three dynamic Australian-born cyber security companies that have successfully moved overseas and are now 'boomeranging' back home. Founders Casey Ellis (Bugcrowd) and Mohan Koo (Dtex Systems), together with Hamish Hawthorn (COO, UpGuard) are passionate advocates for cyber security and for Australia's immense local talent. They agree that by encouraging the domestic market to invest in and procure Australian solutions, there is a significant opportunity to grow the nation's capabilities for economic benefit and establish a globally attractive cyber security ecosystem.

There are common themes threaded through the journey of these companies. Years ago, all left Australia in order to access early-stage capital, be near business mentoring and growth support networks, and grow their customer base.

Bugcrowd is headquartered in San Francisco in the US, with offices in London and Sydney. UpGuard have head offices in the US and Sydney, with offices in Mexico, Spain and New Zealand. Similarly, Dtex Systems have headquarters in Silicon Valley whilst continuing to grow their Australian, US and European business with several offices in Australia and London. All companies built on their overseas success to establish business units in Australia, mostly in research and development, as well as sales support. All are optimistic about Australia's future as a cyber security leader.

Bugcrowd's Casey Ellis sees the Australian market improving for startups, as high-value talent and increasing levels of investor capital start to flow. Ellis recognises Australians have many strengths and that organisations, including Bugcrowd, want access to the 'Australian DNA' that makes the country's cyber security professionals so attractive. 'Australia is world-class at troubleshooting. The world knows it, but Australia doesn't – yet,' says Ellis. Establishing a

presence in Australia is part of Bugcrowd's continuing growth and a positive way to engage in the growing local cyber security ecosystem.

Mohan Koo from Dtex Systems firmly believes Australia is now able to seize opportunities in the global cyber security sector and this will generate economic growth for Australia over the next five to 10 years. 'Australia can be a centre of cyber excellence for the region,' says Koo. For this to occur, he believes the mindset of Australian businesses and government must evolve to be less conservative by encouraging innovation and buying local cyber security solutions. Koo also sees Australian universities playing a crucial role in fostering growth as part of maturing the ecosystem, with Dtex Systems planning to launch a Centre of Excellence in the new Australian Cyber Collaboration Centre in South Australia in 2020.

UpGuard's Hamish Hawthorn is keen to see 'less reliance by large Australian enterprises on traditional suppliers and vendors and a greater willingness to work with Australian technology companies who are solving problems in more innovative ways, in the face of a dynamic cyber risk environment.' He says building a domestic capability is key to developing a vibrant cyber security ecosystem. Hawthorn attributes his time in Silicon Valley as beneficial to developing and strengthening the product UpGuard now offers, largely due to the intensity of the competition in the US market, but also the Silicon Valley ecosystem that encourages fast learning through iterative development of solutions. This process of innovation is something Hawthorn believes Australia can achieve through continued cultural change and greater risk tolerance for emerging technology.
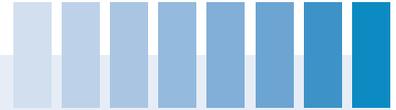
Box 2

BlackBerry: Leveraging AI to help build a trustworthy digital economy in Australia

Australia has an opportunity to play a critical role in maintaining the integrity of communications in our data-driven world. To be globally competitive, the nation must embrace innovative technologies, big data and new skill sets. However, balancing that transformation against evolving cyber threats, data privacy laws and retaining skilled people is an ongoing challenge.

Australia is a key global market for BlackBerry, now a leading artificial intelligence (AI) security software company. BlackBerry is headquartered in Canada, one of Australia's sister nations in the global 'Five Eye' (FVEY) intelligence-sharing alliance. Both nations also share expansive geographies, innovation hubs and rich natural resources – all underpinned by a common goal to protect data, people and industries, while fostering growth. This is a significant driver of BlackBerry's investment in the region.

David Nicol, Managing Director of BlackBerry in Australia, says, 'The intersection of our digital and physical worlds is influencing how Australian organisations approach cyber security and business continuity. Mitigating the human impact of a ransomware-attack in the health sector, for example, requires far more than good cyber policies. It demands fail-safe, secure, real-time communications when something inevitably goes wrong.'

BlackBerry has taken 35+ years of experience in securing millions of smartphones and is now delivering on its mission to secure billions of endpoints. Today, BlackBerry software protects half a billion endpoints globally and this is expanding at pace. To name a few, this includes 150 million vehicles, the NASA space station, traffic control systems, medical devices and power plants.

In Australia, the company helps to protect government and key industries such as finance, energy and education. Customers include: Macquarie University, which uses crisis communications technology to keep staff and students safe; and Melanoma Institute Australia (MIA) and Queensland Investment Corporation (QIC), which use encrypted file-sharing technology to accelerate workplace collaboration and comply with stringent data security and privacy laws. Put simply, BlackBerry provides intelligent security, everywhere, to help enterprises connect, protect and build secure endpoints users can trust.

An important milestone in the company's transformation was the acquisition of AI-cyber security company, Cylance, in February 2019, further bolstering BlackBerry's AI capabilities. Customers like the Sydney Opera House, Reece Group and state and federal government departments are taking advantage of BlackBerry's predictive AI cybersecurity technology to mitigate against next-generation threats and automate tasks, allowing teams to focus on other priorities.

Leveraging new technologies and re-focusing resources is one way to address the cyber skills shortage in Australia, but more needs to be done. Collaboration between government, industry and educational institutions is imperative to foster talent and narrow the gap. That's one of the many reasons BlackBerry was proud to partner with AustCyber for CyberTaipan in March 2019, helping to foster new skills for the next generation of cyber professionals that will lead our workforce.

Nicol's says, '2020 will be a critical year for Australia to develop and implement a cyber policy and practices to effectively address the next generation of threats, boost skills development and accelerate growth. To build a trustworthy digital economy in Australia, we are helping our customers embrace innovation, focus skilled resources in the right areas and maintain data integrity so they can truly benefit from the prosperity that digitisation can bring to industry and society.'

2 THE POTENTIAL: AUSTRALIA COULD BECOME WORLD-LEADING IN CYBER SECURITY

Key points in this chapter

- Cyber security in Australia employs around **20,500** people

- Total expenditure is **A$5.0 billion** in 2018

- More than three-quarters of the market is **dominated by foreign companies**, mostly with local bases employing Australians

- Many local companies are **not harnessing their full export potential**

- **Australia can compete most effectively in software** (in areas of distinctive research capability) and services (in the protection stack and underlying processes)

- **A$3.9 billion** spent on external cyber security 2018

- **A$1 billion** on their internal cyber security functions in 2018

- Small but **fast-growing sector**

- Strong cyber security will **enhance Australia's global reputation** as a trusted and secure place to do business

- **Foundation for future success** of all industries in national economy

2.1 OVERVIEW

Cyber security in Australia is a small but fast-growing sector that is starting to rapidly mature. It is estimated to employ approximately 20,500 people, either as part of an organisation's internal cyber security workforce or through external cyber security providers. Total expenditure on cyber security in Australia in 2018 amounted to approximately A$5.0 billion. Australian demand and employment is dominated by outsourced cyber security services, and more than three-quarters of this market is controlled by foreign companies – though mostly operating from local bases and employing Australians. Software and hardware markets are dominated by direct imports.

Despite this, there are already a number of home-grown cyber security success stories. Australian cyber security providers have developed strong offerings in software and service niches. Several Australian software companies have also joined global value chains and established worldwide reputations for their products. Developments over the last year are particularly promising. Interviews conducted for this updated Sector Competitiveness Plan indicate that procurement officers are increasingly aware of the growing number of Australian cyber security providers with compelling products and services. AustCyber's new initiative GovPitch has contributed to this growing awareness by offering a space for domestic cyber security startups to pitch their solutions to public sector officials and stand a chance to secure a government contract. The cyber security workforce has grown strongly, despite a persistent talent shortage in Australia.

Australia's internationally successful cyber companies have continued to expand, including Bugcrowd, Dtex Systems and UpGuard. Many are building on their international success as a lever to drive further expansion at home.

However, many Australian cyber security service companies are still failing to harness their full export potential. This is at odds with evidence that Australia is considered a services hub, with Australian businesses generally earning much more revenue (relative to national GDP) from services than their peers elsewhere in the world. Cyber security companies could do more to make use of this fundamental country-specific advantage.

2 THE POTENTIAL: AUSTRALIA COULD BECOME WORLD-LEADING IN CYBER SECURITY

Given the small scale of the domestic market, Australia will struggle to become globally competitive in all segments of the cyber security sector. Instead, limited resources should be targeted to parts of the cyber security sector that are both attractive and where Australia can compete most effectively. Analysis suggests this includes:

- **software** – in areas of distinctive research capability
- **services** – in the protection stack and underlying processes.

While these segments will be the initial focus of industry development, many government and AustCyber actions will also support the competitiveness of the industry as whole.

Australia should also consider the opportunity in cyber security to build on other national sector strengths, such as resources and financial services. By building products and services that address the specific cyber security needs of these sectors, Australian companies can develop distinctive, competitive offerings for the global marketplace.

> "
> Cyber security services will likely experience a much stronger growth in demand than cyber security hardware and software

2.2 STRONG LOCAL DEMAND FOR CYBER SECURITY SERVICES

Increasing risk awareness has led companies to invest more heavily in the safety of their networks and IT systems. According to a recent Telstra survey, 84 per cent of Australian companies are planning to increase their overall security spending (cyber and electronic) over the next 12 to 24 months. Only 2 per cent of respondents are planning to decrease their security budgets.[1]

In 2018, total external spending on cyber security in Australia reached A$3.9 billion (see Figure 9) and is expected to remain strong. From 2018 to 2026, external cyber security spending in Australia is likely to increase more than twice as fast (7.9 per cent annual growth) as broader IT spending (3.8 per cent), which was almost A$91 billion in 2018.[2] It is estimated that Australian organisations spent a further A$1 billion on their internal cyber security functions in 2018.

The demand for cyber security products and services in Australia is comparable to global demand trends, but with a larger emphasis on services. Figure 9 shows that around 71 per cent of the local sector's external demand is for cyber security services, compared with around 60 per cent globally. Demand is particularly strong for services that strengthen the operational security of a business or other organisation. The dominance of the services segment in Australia may be partly explained by the particular structure of the local economy, where small and medium-sized enterprises make up around 95 per cent of all Australian businesses. These businesses may lack the scale and resources to run in-house cyber security management teams.

Over the next decade, the current demand pattern is set to intensify as organisations are expected to make even greater use of outsourced services to manage growing security needs and a proliferation of security breaches. It means that cyber security services will likely experience a much stronger growth in demand than cyber security hardware and software. This basic trend applies to both Australia and the world, but in Australia the additional demand is expected to bolster a broad spectrum of different security services – from the protection stack to underlying processes – whereas globally demand is expected to strengthen most notably for security operations services.

---

1   Telstra (2019), *Telstra Security Report 2019*.
2   Which 50 (2017), 'Australian IT Spend Nears $87 Billion: Gartner'. Available at: **https://www.arnnet.com.au/article/660273/australia-it-spending-reach-94b-2019/**.

Figure 9

Breakdown of Australian external cyber security spend

Millions A$, 2018

Larger ■■■■■ Smaller

Product type*	Security need			Total
	1 Protection stack	**2** Security operations	**3** Underlying processes	
Hardware	$135 M	$30 M	N/A	$165 M
Software	$540 M	$360 M	$89 M	$990 M
Services	$1,150 M	$1,195 M	$440 M	$2,785 M
Total	$1,825 M	$1,585 M	$530 M	$3,940 M

Australia's demand is even more heavily weighted toward services than the world overall, potentially driven by increased outsourcing – Australia has relatively fewer companies of the scale required to conduct security activities in-house

Note: Figures rounded to the nearest A$5M

* Hardware refers to physical devices (e.g. firewalls); services includes consulting, MSS, implementation and support services

Source: Gartner; IDC; expert interviews; AlphaBeta and McKinsey analysis

2.3 MUCH OF LOCAL DEMAND IS MET BY FOREIGN COMPANIES

Foreign providers meet much of the existing domestic demand for cyber security products and services. For example, currently there are no local companies among the 15 largest software providers by value in the Australian cyber security market. The combined market share of Australian companies is estimated to be less than five per cent. It is a similar picture in hardware, with no major Australian hardware providers. The representation of Australian companies is stronger in services. Noting that the market data is not strong, interviews and other sources suggest the market share of Australian home-grown services companies is about

25 per cent, while around half of the market is served by foreign-owned companies with core personnel in Australia (this excludes foreign companies with only a sales presence in Australia).[3]

Putting these findings together provides a view of Australia's cyber security sector revenue – defined as the revenue from the sale of cyber security products and services by businesses with a core team in Australia.[4]

Figure 10 shows that Australia's cyber security sector generated around A$2.6 billion in revenue in 2018 (see Appendix B for details of the methodology and assumptions).[5]

Figure 10

Breakdown of Australian external cyber security spend

A$M, 2018

Imports refer to earnings of foreign providers serving Australian customers **without having a core team in Australia**, for example:
• A foreign software provider selling software to Australian organisations, with only a sales team in Australia
• A managed security service provider operating a security operations centre from abroad

Exports refer to earnings from **serving foreign customers**. Includes earnings of all providers with core teams in Australia, for example:
• An Australian software firm selling software to foreign customers
• International students studying cyber security in Australia

~3,900 ~1,700 ~400 ~2,600

Australian external cyber security spending   Imports*   Exports*   Australian cyber security industry revenue

Note: Figures rounded to the nearest $100M.
* Imports and exports are rough estimates only and are based on interviews with Australian industry stakeholders across each product type
SOURCE: Gartner, IDC, IbisWorld, stakeholder interviews, AlphaBeta and McKinsey analysis

3   Services are more likely to be provided locally due to the lower exportability of cyber security services compared with hardware and software.
4   Estimating sector revenue requires subtracting imports (defined in this context as cyber security products and services provided from abroad, without core personnel in Australia), and adding exports (defined as revenue obtained from serving foreign customers from Australia). This definition captures all the revenues that contribute to Australian cyber security employment.
5   Estimating gross revenue or value added for the cyber security sector is difficult because of the lack of sector-specific data on cyber security collected by the Australian Bureau of Statistics. Cyber security, for example, does not appear in the Australian and New Zealand Standard Industrial Classification, which is used for the compilation of industry statistics in Australia. One cyber security-related profession, ICT Security Specialist, occurs at the 6-digit level of the Australian and New Zealand Standard Classification of Occupations, but little employment data is collected or reported at this low level.

There are important signs over the last two years that the local sector is maturing. The pace of mergers and acquisitions across the sector is increasing, with the acquisition of Hivint by Singtel, Aleron by EY, SmartEncrypt by Rhipe and the recent creation of CyberCX, which combines 12 Australian cyber security services firms under a single brand. The flow of capital into cyber security in Australia also appears to be improving, with a number of Australian firms completing significant capital raisings during 2018 and 2019, including archTIS, Cloud Conformity, Kasada, Secure Code Warrior and Vault Cloud.

While employment in cyber security in Australia has increased above 20,500 in the last year, limited availability of skilled workers is still a significant challenge constraining the growth of the sector (see Chapter 3 for further details on the skills challenge).

Government, educational institutions and industry are working hard to ramp up cyber education and training but it will take some time for the impact of these initiatives to be observed in workforce growth.

Foreign service providers with local operations remain the largest employer in Australia's external cyber security market (as seen in Figure 11). Multinational corporations currently employ around 7,000 cyber security workers. Since many services are difficult to import directly (for reasons discussed in the previous chapter) and need to be provided through local operations, these companies make a very significant contribution to the overall workforce. They are only exceeded by internal employment of cyber security teams, which is estimated to be around 9,000 workers.

Figure 11

Breakdown of cyber security employment in Australia by type of firm*

jobs in 2018, estimates only and rounded to the nearest 500 workers
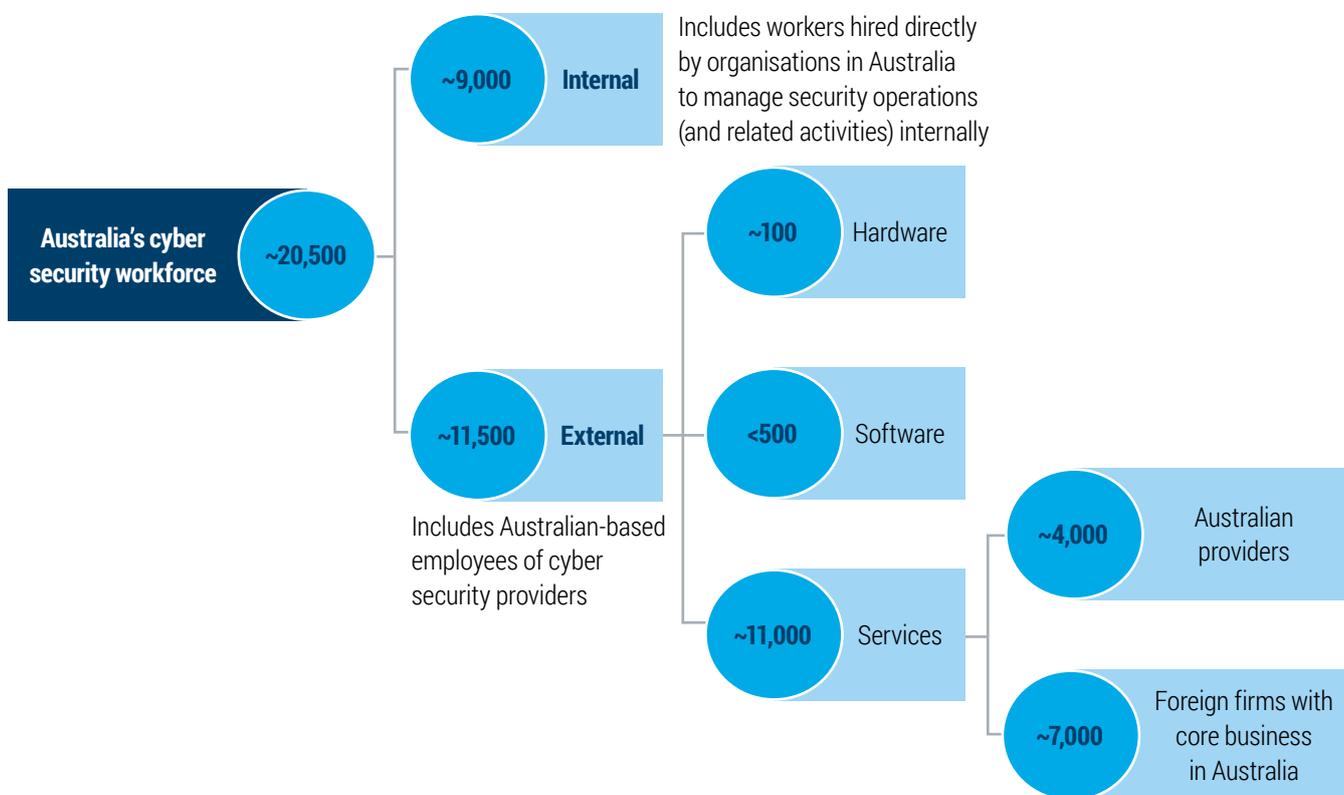
Note: Components may not sum to totals due to rounding

*   External jobs based on revenue and revenue-per-job estimates; internal based on global internal spending data as a proportion of total spending, adjusted based on survey results suggesting Australia outsources to a greater extent than the global average. Includes direct labour only (excludes non-cyber security professions in other industries supported indirectly by cyber security)

SOURCE: Gartner, Australian Bureau of Statistics, stakeholder interviews, AlphaBeta and McKinsey analysis

2 THE POTENTIAL: AUSTRALIA COULD BECOME WORLD-LEADING IN CYBER SECURITY

2.4 LOCAL CYBER SECURITY COMPANIES ARE COMPETITIVE IN SOFTWARE AND SERVICES

Australian companies have been successful in areas of both software and services, in both domestic and international markets.

Software

In software, there is a strong 'beachhead' of Australian companies in the area of security operations. Companies such as Covata, StratoKey, Airlock Digital, Kasada and Huntsman have developed successful software products and established market presence both in Australia and in international markets.

Australian cyber security software companies are also exporting their products in the protection stack area (for example, Mailguard) and in the area of underlying processes (for example, Secure Code Warrior).

Hardware

The representation of local companies in hardware is weaker, although the innovative work of Penten (see Box 4), QuintessenceLabs (see Box 14), Amplify Intelligence and Serinus Security demonstrates that Australian companies can still play a strong role in niche areas of hardware.

Box 3

ArchTIS: Canberra-based tech company tackles the information sharing trust deficit

One of the most challenging issues facing government and industry in a digital age is how to securely share sensitive, valuable and classified information. While sharing information comes with benefits for productivity and service outcomes, it does come with risks. Malicious actors and cyber criminals are targeting this information, which can threaten national security and lead to financial and reputational harm.

archTIS was founded in 2006 to solve this global critical problem. The company built its credentials in the TOP SECRET information environment, with various consulting contracts in Australia and abroad.

One of these contracts included building an information sharing and collaboration platform for Defence, which would enable users to share TOP SECRET/SCI classified information between Australia and the United States. The platform did this using a revolutionary tagging method, based on Attribute Based Access Control (ABAC).

archTIS saw a broader need for collaboration of classified information across government, particularly at the federal level. The company raised private and eventually public equity to develop the fourth generation of the platform for government to government and government to industry collaboration at the PROTECTED level.

This platform is now available as a Digital Transformation Agency (DTA) assessed cloud service, and as an on-premise (Kojensi Enterprise) or deployable platform (Kojensi Field) for collaboration up to TOP SECRET.

The key benefit of this platform is its multi-level security model, enabling it to host information of varying classification levels where each user accesses only what they are entitled to access.

Since launching in April 2019, archTIS' Kojensi platform has been met with strong demand and understanding in Australia and abroad.

archTIS has:

- successfully listed Kojensi Gov on the DTA's Cloud Marketplace;
- been invited to NATO to demonstrate the platform to NATO Communications and Information Agency staff;
- deployed the platform to the company's first client – Australia's Attorney General's Department;
- entered the intelligence and law enforcement market, selling to the Australian Criminal Intelligence Commission; and
- expanded to New Zealand with a reseller agreement with local company Team Asparona.

The company sees its uses expand well beyond government, including the Defence supply chain, multi-coalition collaboration and universities conducting research for government and Defence.
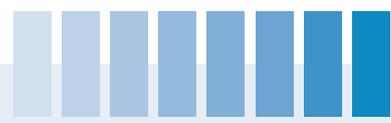
Box 4

Penten: Cyber deception for trapping attackers and high-grade encryption for mobility

For Penten, the last 12 months have been about scaling up, managed services, and yet more growth and innovation, including:

- signing major projects, including with Defence;
- growing their customer base in Australia and the UK;
- increasing staff numbers from 50 to 75;
- experiencing a 100 per cent revenue increase for the third consecutive year; and
- launching two new products – the AltoCrypt Phone and TrapAir (a WiFi honeytrap).

At the release of AustCyber's first Sector Competitiveness Plan in 2017, Penten also launched AltoCrypt Stik – its flagship secure mobility product for Defence and other government agencies. Penten's AltoCrypt Stik is a secure, small and discreet USB device that enables government users to access highly classified networks wirelessly, both in the office and remotely. AltoCrypt Stik has been described as the game changer for access to classified information, and Penten has secured significant government contracts to deliver the capability, including to Defence via the Defence Innovation Hub.

In 2019, Penten rebranded their new Applied Artificial Intelligence (AI) business unit in response to growing customer demand. The team has commenced several new partnerships with international and local businesses to expand cyber deception offerings. Their AI expertise is used to support cyber training, testing and automation. These new offerings include Honeytrace (a joint offering with Australian startup WorldStack) to detect data theft of customer and business records, and TrapAir, an innovation that mimics your WiFi hotspots to detect malicious interactions with your computer networks.

AustCyber has provided customer introductions, mentoring and market awareness opportunities to Penten. 'AustCyber has encouraged us to work with other Australian cyber businesses to create more complete and compelling offerings,' says Penten's CEO, Matthew Wilson. 'Our partnership with QuintessenceLabs was born out of collaboration opportunities created by AustCyber.'

Penten continues to grow its security cleared and highly experienced team – adding project managers, logistics and finance professionals – along with significantly growing its hardware, software, networking and security engineering capabilities. Penten has focused heavily on building the team, processes and artefacts to shape Australian solutions ready for export. The outcomes enable customers to solve their challenges with world leading capability that can be simply transitioned into service.

Services

The services segment of Australia's cyber security sector contains a large number of local companies. In the protection stack, Australian companies such as archTIS and Shearwater Solutions provide services in security architecture and penetration testing. Security operations are dominated by service providers managed by large multinationals, but does include some smaller Australian companies including Telstra.

Australia is strongest in the third security need area of underlying processes. In addition, Australia's universities and TAFEs are increasingly participating in the services segment by providing cyber security courses designed to train students for work in the sector (see Box 9 for details).

An increasing number of local companies are exporting their services, with particular success in the Indo-Pacific. Among those that do have a significant presence abroad is Bugcrowd (see Box 1). The company was founded in Australia in 2012, but has since shifted its headquarters to San Francisco, partly for better access to venture capital. Telecommunications company

Telstra has ventured into Southeast Asia, through a partnership with Telkom Indonesia, comprising a jointly managed data network and security services. Other examples of cyber service providers with large international operations include risk-analysis company UpGuard and endpoint-protection company Dtex Systems. Both were founded in Australia but, similar to Bugcrowd, are now headquartered in the US. Some Australian universities also 'export' education by offering cyber security courses to international students.

Revealed competitive advantage

The concept of revealed comparative advantage (RCA) can help identify country-specific strengths by measuring an economy's current supply of a product or service against the backdrop of global supply. It measures how much more or less successful that country is than the world average when supplying a particular good or service. An RCA index value above 1 signals that a country enjoys a comparative advantage in the supply of a certain product or service. In contrast, an index value below 1 indicates a disadvantage relative to other suppliers globally.

Figure 12

Revenue and advantage

Revenue over GDP by segment and region*

US$M in revenue per US$ trillion of GDP
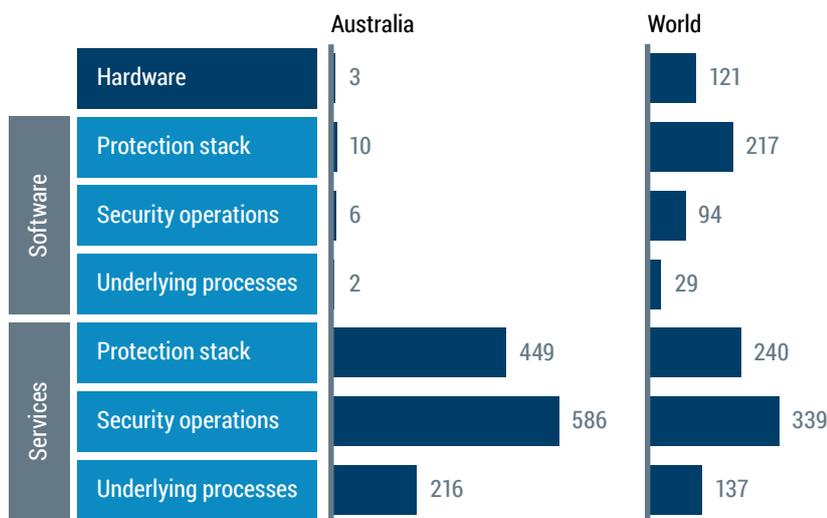
Australia's revealed comparative advantage†

Index, Australia/World

1 = Parity with world

	Australia	World	Index (Australia/World)	
Software				
Hardware	3	121	0.08	Australia significantly under-indexes in hardware and software, across all security needs
Protection stack	10	217	0.16	
Security operations	6	94	0.22	
Underlying processes	2	29	0.20	
Services				
Protection stack	449	240	1.62	Australia over-indexes in services across all security needs
Security operations	586	339	1.47	
Underlying processes	216	137	1.44	

* Revenue to Australia includes revenue to firms with core operations in Australia. Includes estimates of export revenue (based on interviews with industry)

† Revealed comparative advantage is calculated as the Australian industry size in a given segment over Australian GDP divided by the worldwide segment size over global GDP. An index value above 1 suggests that Australia has a comparative advantage in a particular segment

SOURCE: Gartner; World Bank WDI Database; UN World Input-Output Table; AlphaBeta and McKinsey analysis

The analysis in Figure 12 reveals that Australian companies and foreign companies with core operations in Australia already earn much higher revenue (relative to national GDP) in services than their average peers worldwide. This highlights a substantial comparative advantage in the services segment of the cyber security sector. The situation, however, is reversed in the hardware and software segments, where the current revenues (relative to national GDP) of Australian companies and foreign companies with core operations in Australia are significantly lower than the equivalent world average, signalling a comparative disadvantage.

2.5 AUSTRALIA'S OPPORTUNITY: FOCUS INITIALLY ON A LIMITED NUMBER OF SEGMENTS

Australian cyber security companies have proven to be successful abroad, even in highly competitive markets such as the US and Europe. To emulate the success of these local 'pioneer' companies across the wider Australian cyber security sector, Australia needs to identify and focus on its country-specific competitive advantages. The talent base and resources also need to be developed to turn Australia's strengths into a competitive edge. While the role of AustCyber is to promote and improve the competitiveness of the entire cyber security industry, it will also support the development of several initial focus segments.

In developing this updated Sector Competitiveness Plan, a rigorous framework of analysis was used to identify several segments within the Australian cyber security sector that promise the largest opportunities for the Australian economy over the next decade. Seven segments appear most noteworthy – three software segments and three services segments meeting the

Figure 13

Cyber security sector segments assessed on attractiveness and Australia's ability to compete
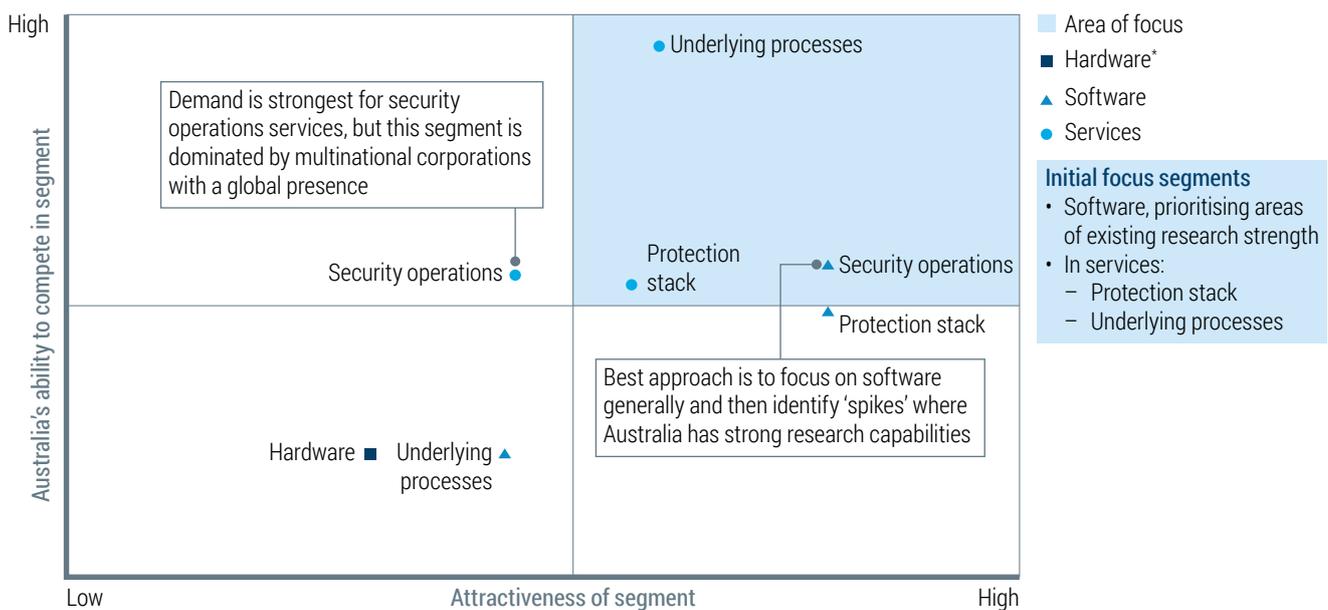
*   Hardware has been considered as one segment because it is significantly smaller than the other product types and heavily concentrated in the protection stack
SOURCE: AlphaBeta and McKinsey analysis

three basic security needs (protection stack, security operations and underlying processes), and one segment for hardware. To understand which of these segments warrant the greatest initial focus, they were analysed according to their:

Attractiveness – This is based on the segment's size and growth internationally and in Australia, its exportability, its potential to create jobs and the quality of those jobs, and its fit with technological trends.

Competitiveness – This is based on Australia's ability to compete, considering existing presence, any revealed comparative advantage, and the segment's match with Australia's skill profile.

As a result of this analysis and tested through extensive interviews with industry participants, three focus segments stand out: software (prioritising areas of existing research strength), services in the protection stack, and services in underlying processes.

Software

Software is an attractive segment in both security operations and the protection stack. It has a strong existing presence in the protection stack and the largest forecast increase in demand for security operations. Software products are highly exportable and generate high-quality jobs. The convergence of IT and OT, mobile internet and the Internet of Things will also have a positive effect, multiplying the complexity of networks and security operations. Automation is also likely to emphasise software at the expense of services, as developments in AI and advanced machine learning lead to more sophisticated software-based solutions.

Given the appeal of both these areas for software, the best approach for Australia is to consider software as one broad segment and then identify specific areas of research capability to build on for a strong software ecosystem. Two possible areas of focus are cryptography (which is typically applied in the protection stack) and data analytics (in security operations). However, these will need to be further refined through more detailed assessment of Australia's comparative research strengths.

Though software is an attractive segment, it is not as strong in terms of competitiveness – the evidence is not as strong for Australia's ability to compete effectively in software. Australia's current revenue in software is very low, which implies a lack of comparative advantage. However, several companies have succeeded both domestically and in export markets. These include Huntsman and Stratokey. These 'beachhead' companies can provide a model for the development of a stronger Australian software segment.

Services – protection stack

The protection stack includes a range of services that protect organisational networks, applications and endpoints from malicious attackers (see Box 5 for an example). Specific services include network security architecture, firewall configuration and management, penetration testing, vulnerability assessment, and patch and configuration management. Services in the protection stack currently comprise the second largest segment in the Australian industry – after services in security operations – and this area is forecast to experience continued strong demand growth.

While harder to export than software, protection stack services are still relatively exportable due to less need for in-country technical teams to provide the services than is the case in security operations. It requires a strong supply of medium- to high-skill workers, which matches well with the skill profile of the Australian cyber security workforce. The convergence of IT and OT along with the Internet of Things are two trends that increase the number of network endpoints and the need to protect them. Automation may have some negative impact on employment in the protection stack services market, but the strong outlook for demand growth means the negative effect should remain limited.

Australia already has a strong competitive advantage in cyber security protection stack services

In interviews, many CISOs and CIOs say services such as penetration testing and network security architecture are currently Australia's most outstanding segments in the cyber security sector. Australian companies are already successfully exporting these services. Mailguard, for example, has developed an email and cloud security service that is now sold in 27 countries worldwide. Mailguard's solution builds on a platform of 'Software as a Service' (SaaS) to create what is effectively a niche-managed service providing email filtering.

Box 5

ResponSight: Identifying cyber risks in new ways

ResponSight is an Australian data science company focused on delivering behavioural reputation and risk insights using only statistical and telemetry data, while avoiding the collection and storage of risky sensitive or private information.

While traditional systems actively search for cyber threats, ResponSight focuses on monitoring a person's typical behaviour by collecting numerical, mathematical and statistical data with the help of cloud-based analytics engines. ResponSight consolidates and analyses metrics usually ignored by traditional technologies to understand a user's 'behavioural fingerprint', that is a unique, nuanced way of how people use their computers.

ResponSight says its approach is more innovative than many other approaches that analyse user behaviour by relying on incomplete or inaccurate log data or centralised Security Incident and Event Management repositories. It says endpoint analytics collected in this new way allow it to create behavioural fingerprints that provide insights not available in existing technologies. ResponSight's approach allows organisations to improve the value of their existing investments, and potentially reduce time and effort associated with alert management and incident investigations.

Founded in 2015, ResponSight has partnered with a national advisory firm to deliver technology and services in incident response and forensics, with plans to expand its customer base into the US in 2020. ResponSight was part of trade missions to San Francisco in 2017 and 2018, jointly organised by AustCyber and Austrade.

Services – underlying processes

Organisations seeking to increase the security of underlying processes can choose from various services, including the development of cyber security strategies, risk and compliance policies, employee training, and measures to raise the general awareness of cyber security risks (see Box 6 for one example). Services to improve underlying processes represent about 16 per cent, or A$421 million, of the total external spending on cyber security services in Australia (see Figure 5).

The exportability of services varies considerably. Governance, risk and compliance, for example, is challenging to deliver without having a strong technical team on the ground that understands a country's regulatory environment. In contrast, awareness, training and oversight services can be delivered remotely. Cyber security training appears particularly well suited for exporting, as it can be offered online or through international student enrolments.

Education-related travel services are now Australia's largest non-resource export, generating A$28 billion in the fiscal year 2017, or 7.5 per cent of total export revenues.[6] The quality of Australian education is highly regarded abroad, particularly in the Indo-Pacific region. As continued strong global growth in cyber security creates demand for skilled professionals (see Chapter 4 for details on skills shortages), Australia's experience in export of education means the nation's universities and vocational training institutions are well positioned to exploit this opportunity. Several universities and training institutions are already active in this segment and report a high number of international students in cyber security programs, especially in Masters study programs.

Similarly, Australia already has a strong ecosystem of local companies offering cyber security governance, risk and compliance services. While most have not yet attempted to export these services, some are currently exploring more scalable service delivery models that may enable exportability. Cyber security company Hivint, for example, has established an innovative service platform Security Colony which it is now launching in the US through the Australian Landing Pad Program.

6   Austrade (2017), 'Australia's export performance in FY2017'. Available at: https://www.austrade.gov.au/news/economic-analysis/australias-export-performance-in-fy2017.

Box 6

Airlock Digital: Keeping cyber intruders at bay

Airlock Digital, an Australian company founded in 2013, helps keep cyber intruders out of an organisation's network by enabling organisations to implement application whitelisting.

Application whitelisting is the practice where organisations specify which applications (such as programs, software libraries, scripts and installers) are trusted, while blocking everything else by default. This strategy is recognised by the Australian Signals Directorate as one of the most effective strategies to mitigate against malicious cyber security incidents.

But what sounds simple in theory, is often a challenging endeavour for both small and large organisations. Airlock Digital exists to solve this challenge, offering application whitelisting solutions focused on ease of implementation, incorporating workflows that align to the customers' existing business processes.

Unlike signature-based file blocking (blacklisting) such as antivirus software, Airlock Digital's solution proactively sets up barriers to ensure attackers cannot execute malicious and unknown code. Airlock then verifies, monitors and records all file executions, permitting only authorised files to run in customer environments. This makes the solution extremely effective at preventing both opportunistic and sophisticated attacks, including ransomware. Airlock Digital provides customers with proactive security that reduces the need for incident response and provides insight into the files and scripts that exist within their organisation.

Airlock Digital application whitelisting has proven effective in many industries – including government agencies, critical infrastructure, large enterprises, education and small business both domestically and abroad. Airlock has recently accelerated their business by partnering with CrowdStrike to deliver application whitelisting through the CrowdStrike platform internationally in 2020.

1. Baseline

– Capture a SOE

2. Capture

– Create policies
– Monitor
– Capture applications

3. Enforce

– Secure endpoints

These three segments – software, services in the protection stack, and services in underlying processes – will be the initial focus of efforts to develop a globally competitive Australian cyber security sector. However, many of the strategies and actions proposed for AustCyber and others to support of these segments will also benefit the wider cyber security industry. AustCyber will regularly review the set of focus segments to respond to changes in the industry structure and technology trends that have not been anticipated.

2 THE POTENTIAL: AUSTRALIA COULD BECOME WORLD-LEADING IN CYBER SECURITY

2.6 PLAYING TO AUSTRALIA'S STRENGTHS

Australia's most promising opportunities in cyber security, while driven primarily by the attractiveness and feasibility of the different product types and security needs, should also consider opportunities emerging from the varying needs of different industries that use cyber security.

While all industries have the same basic security needs, the specific cyber security threats they face – for example, protecting large quantities of confidential user data or hardening the resilience of operational technology – informs the specific mix of products and services required. This means there are potential sources of comparative advantage for Australian companies in the industry composition of Australian cyber security demand, the industry mix of the broader economy, and in the nation's export performance.

The Australian Cyber Security Industry Roadmap, jointly developed by CSIRO Futures, Data61 and AustCyber, specifically identifies growth opportunities at the intersection of cyber security and Australia's five other priority growth sectors: medical technologies and pharmaceuticals; mining equipment, technology and services; advanced manufacturing; oil and gas; and food and agribusiness.

One other example of such industry strengths is financial services. Australia's financial services companies are the largest users of cyber security in the country. They account for almost one-third of the nationwide security demand, which means they are a much more relevant customer group for cyber security providers in Australia than financial services companies are elsewhere in the world, as illustrated in Figure 14. Financial services organisation face some of the most challenging threats to their cyber security, as the convenience of modern consumer banking – featuring ATMs, point-of-sale systems and mobile banking – has vastly increased the number of endpoints that need to be protected. Banks are also responsible for some of the most sensitive consumer and corporate data, and risk serious reputational damage in case of a breach.

Cyber security companies could harness Australia's strength as a regional banking and finance hub by tailoring their products and services to the specific security needs of financial services companies. This would allow them to quickly build scale and reach international markets. Interviews with successful Australian cyber security companies revealed several have pursued this strategy effectively. The financial services sector can also play a valuable role through investment in, and becoming an anchor customer for, Australia's cyber security startups. Westpac, for example, has invested in both QuintessenceLabs (Box 14) and Kasada (Box 7) over the past two years.[7] The most recent investment in Kasada demonstrates a large market opportunity for the financial services sector to help scale cyber security products that their customer base can then also adopt.

---

7   *Australian Financial Review* (2017), 'Westpac's Kasada deal points to cyber security as a service'. Available at: http://www.afr.com/business/banking-and-finance/financial-services/westpacs-kasada-deal-points-to-cyber-security-as-a-service-20180324-h0xx9h.

Figure 14

Cyber security external spending by industry scaled for size of economy

US$M in revenue per US$ trillion of GDP

	Australia	World	Difference
Financial services	363	188	175
Federal Government	153	29	125
Telecommunications	131	41	91
Education	68	18	50
Local Government	86	48	38
Professional Services	47	16	32
Transportation	53	51	3
Utilities	51	60	-9
Retail	53	63	-11
Media	37	48	-11
Manufacturing	96	113	-17
Wholesale	16	36	-20
Resources	41	72	-31
Consumer Services	5	40	-35
Healthcare Providers	53	88	-35
Construction	5	43	-38

Australia over-indexes on cyber security spending in several industries
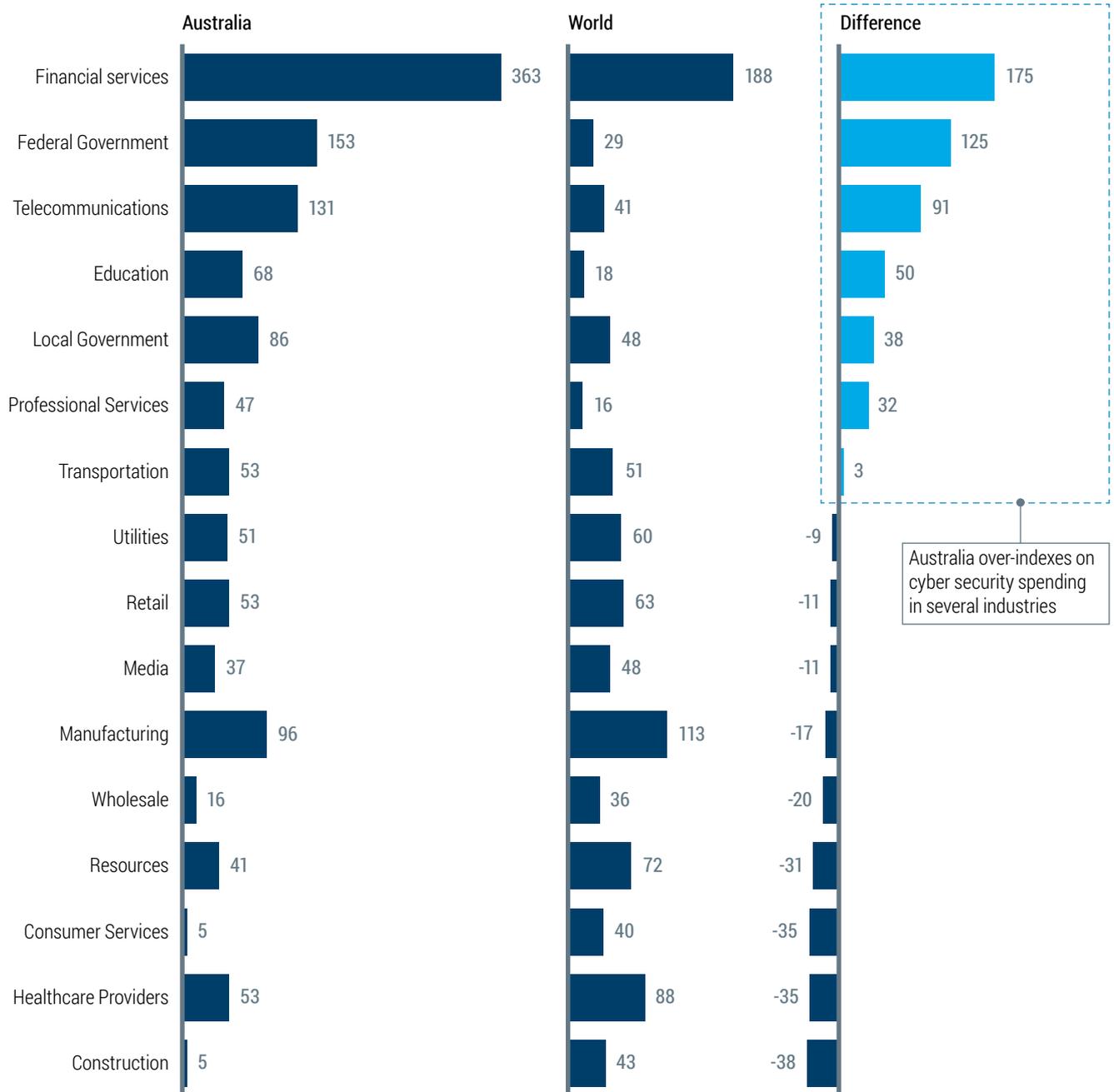
2.7 SIZE OF THE PRIZE: AUSTRALIA'S CYBER REVENUE COULD MORE THAN DOUBLE BY 2026

Australia could harness substantial benefits from developing a globally competitive cyber security sector – even beyond the strong forecast growth in the industry over the next decade. 'Business-as-usual' forecasts imply revenues in the Australian cyber security sector could more than double from A$2.2 billion in 2016 to $4.7 billion in 2026, as shown in Figure 15.

However, the growth potential is even bigger if Australia undertakes concerted actions to support the three initial focus segments – software, services in the protection stack, and services in underlying processes. In this case, revenues in the domestic cyber security sector could increase to A$6.0 billion in 2026, which equates to an annual growth rate of almost 11 per cent over the decade.

If Australia undertakes concerted actions to support the three initial focus segments, revenue could increase to $A6 billion in 2026

Figure 15

Forecast cyber security external revenue growth between 2016 and 2026*

A$M

Legend: ■ Software   ■ Services – Protection stack   ■ Services – Underlying processes

- 2016 revenue: 2,200
- Business-as-usual revenue growth: 2,500
- 2026 business-as-usual revenue: 4,700
- Potential uplift in target segments†: 1,300 (Software 500, Services – Protection stack 600, Services – Underlying processes 200)
- Potential 2026 revenue: 6,000

Revenue growth of +A$3.8B (10.6% CAGR)
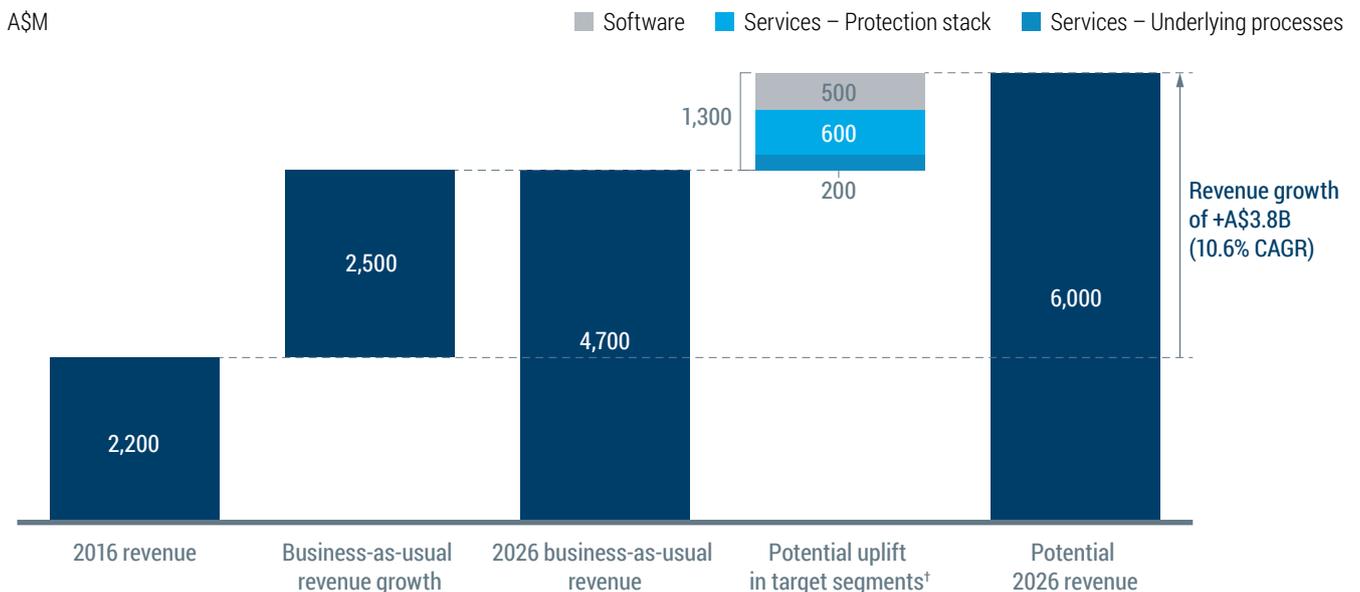
* Revenue attributable to Australian firms and foreign firms with local operations in Australia; based on Gartner market size forecasts, import/export assumptions (informed by stakeholder interviews) and estimates of job intensity

† Potential uplift in focus segments calculated as an average of several benchmarking approaches

SOURCE: Gartner; ABS; stakeholder interviews; AlphaBeta and McKinsey analysis

This revenue growth would generate new jobs in the Australian cyber security sector. 'Business-as-usual' forecasts, illustrated in Figure 15, suggest employment could increase by 7,500 jobs – from 19,000 in 2016 to 26,500 in 2026.

However, the job potential is significantly greater (see Figure 16). If Australia takes decisive action to develop the three focus segments in the cyber security market, in which it already has a competitive advantage, a further 5,100 cyber security jobs could be created. To reach this workforce growth goal of 12,600 more jobs, workers lost from the sector through natural retirement and workers moving overseas will also need to be replaced. The workforce could grow even further if Australia can address the current skills shortage, as discussed in more detail in Chapter 3.

This growth potential is substantial but may still be relatively conservative, as it is based on 'business-as-usual' forecasts and assumes modest improvements in the three focus segments. The performance of leading countries globally in cyber security sector development shows that, if aspiring to global leadership in cyber, Australia could target a much larger sector and workforce by 2026. If Australia could match the performance of global leaders such as the US and Israel, the cyber workforce would expand to almost 60,000 with industry revenue of $11 billion in 2026.[8]

Figure 16

Forecast cyber security workforce growth between 2016 and 2026*
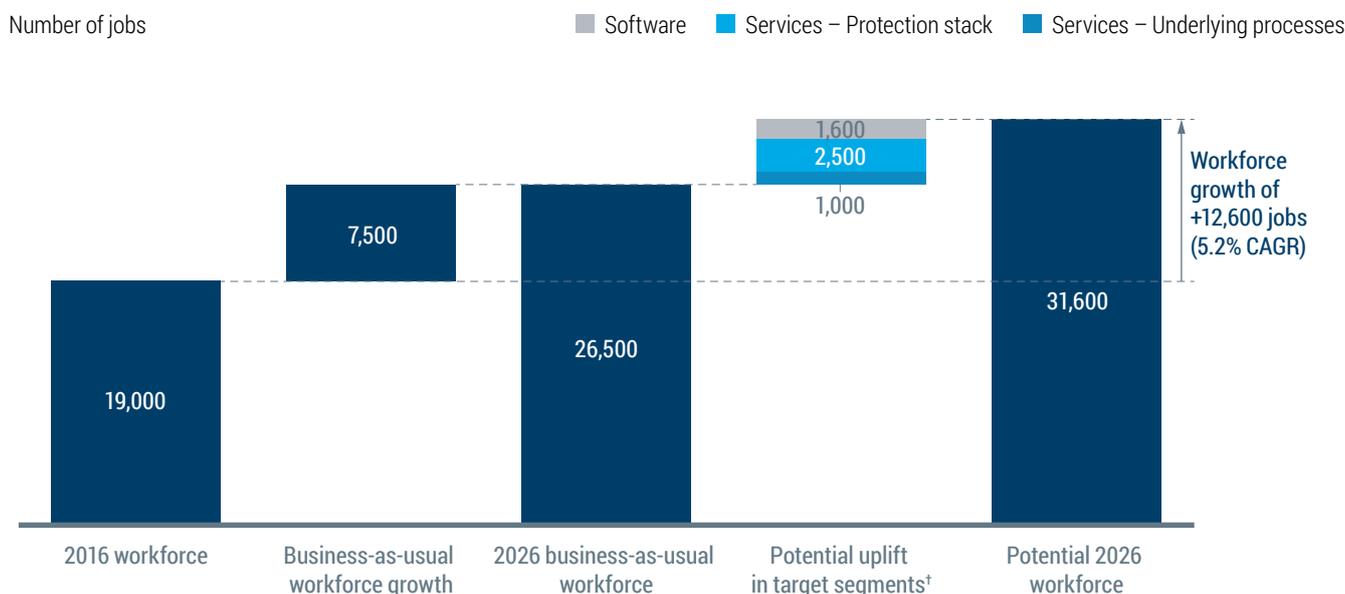
Number of jobs

*   Based on Gartner market size forecasts, import/export assumptions (informed by stakeholder interviews) and estimates of job intensity
†   Potential uplift in focus segments calculated as an average of several benchmarking approaches
SOURCE: Gartner, ABS, stakeholder interviews, AlphaBeta and McKinsey analysis

8   Given the lack of standardised data globally about the size of different countries' cyber security workforces, direct comparisons are difficult. Available data indicates that the US and Israel have around 200 to 250 cyber workers per 100,000 people. In Australia that number is around 80, and the potential 2026 workforce identified in Figure 16 would bring that to around 120 per 100,000. For more information see CyberSeek (2018), *Cybersecurity Supply Demand Heat Map*, available at: http://cyberseek.org/heatmap.html and Haaretz (2017), 'Israel at Risk Amid Shortage of Cyber Security Experts', available at: https://www.haaretz.com/israel-news/business/israel-at-risk-amid-shortage-of-cybersecurity-experts-1.5491404.

Cyber investment also has large spillover benefits

Developing a globally competitive cyber security sector in Australia will have significant spillover benefits to the wider economy. Strong cyber security will enhance Australia's global reputation as a trusted and secure place to do business, increasing demand for other Australian goods and services exports. This is because cyber security is not only a 'vertical' sector in the economy, but a critical 'horizontal' enabler of activity across other sectors. Without strong cyber security, organisations cannot safely and effectively digitise their operations and realise the significant growth benefits that flow from investments in ICT.

Strong cyber security will enhance Australia's global reputation as a trusted and secure place to do business

Analysis of the global benefits and costs of different cyber scenarios provides some sense of the potential impact of cyber security on Australia's broader economy. Research for the Atlantic Council found that cyber security expenditure, while a significant annual cost to the global economy for many years to come, support investments in ICT that yield massive cumulative benefits over the long-term. In Australia, the difference between strong cyber leading to a positive future, and weak cyber leading to lack of trust and investment, could be more than 1 per cent higher GDP by 2026. In the worst-case scenario, where cyber attacks generate constant and widespread disruption to ICT usage, Australia's GDP could be more than 5 per cent lower in 2026 than the base case. This modelling, while based on global rather than national scenarios, demonstrates that cyber security is a critical driver of growth.

However, the role of cyber security in enabling growth is still not well accepted. A 2016 Cisco survey by of senior executives across 10 countries including Australia, found that only one-third believed the primary purpose of cyber security is to enable growth.[9] The remaining two-thirds still viewed cyber security as principally for risk reduction. Less than half perceived cyber security as a source of competitive advantage for their organisation. Further research to understand the impact of cyber security on the growth outlook of the Australian economy could help to change this mindset and support appropriate investments in cyber capability by Australian organisations.

There are also signs that senior executives are beginning to change their understanding of cyber security from risk mitigation to strategic opportunity. In a survey conducted in 11 countries including Australia for KPMG's 2019 Global CEO Outlook, 71% of CEOs said they now see cyber security as a strategic function and a source of competitive advantage.[10] This is markedly higher than previous surveys have found.[11] Further research to understand the impact of cyber security on the growth outlook of the Australian economy could help foster this emerging mindset and support ongoing investments in cyber capability by Australian organisations.

9   Cisco (2016), *Cybersecurity as a growth advantage*. Available at: **https://www.cisco.com/c/dam/assets/offers/pdfs/cybersecurity-growth-advantage.pdf**.

10   KPMG (2019), Agile or irrelevant: 2019 Global CEO Outlook. Available at: **https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/05/kpmg-global-ceo-outlook-2019.pdf**.

11   Cisco (2016), Cybersecurity as a growth advantage. Available at: **https://www.cisco.com/c/dam/assets/offers/pdfs/cybersecurity-growth-advantage.pdf**.

Box 7

Kasada: Youth and innovation stopping malicious web bots

Sam Crowther, the now 24-year-old founder of Australian cyber security startup Kasada, has developed a 'road spike' tool to stop fast moving cyber attacks, called Polyform. The tool foils malicious internet bots by bombarding them with irritating tasks until they give up.

Bots are pieces of code that cyber criminals use to dupe online customers. Wherever people sell something desirable online, bots are usually not far away. For example, they enter the websites of ticketing agencies, e-commerce shops and hotel chains to manipulate their content, pretending concert tickets, limited-edition sneakers or luxury rooms are sold out. Then they offer the same product on eBay and other marketplaces for a higher price, cashing in on the difference. Anyone completing online transactions is susceptible to bots and malicious automation.

It usually only takes bots a few seconds to do the damage, as cyber adversaries have now automated their assaults. They let thousands of bots simultaneously attack websites, leaving traditional cyber defences overwhelmed.

'There's so much power in the code, and automation is ubiquitous,' says Crowther, who as a high school student gained critical work experience with cyber teams at the Department of Defence and Macquarie Group. At just 19 years old, he discovered that blocking malicious code from entering a website is much more effective than trying to destroy it. 'The solutions people have used so far against bots are nothing more than a band-aid,' says Crowther. 'Cyber criminals are increasingly using sophisticated automation to launch attacks, which is why automation is key to staying ahead of the threats.'

Polyform detects and mitigates malicious bot traffic that other security measures are unable to identify. The security Software-as-a-Service offers strategic protection on a

massive scale against attacks on websites, mobile apps and APIs, including account takeovers, data-scraping and other unwanted automated activities. With a time to value of under 30 minutes, Kasada offers a unique, cost-effective solution to bot attacks that improves network bandwidth saturation, computing infrastructure costs and digital marketing ROI.

Kasada's defence strategy proved so successful that it's now trusted by ASX 100, Forbes Global 2000 and mid-sized enterprises in Australia, the UK and US.

Craig Templeton, Chief Information Security Officer at realestate.com.au, appreciates the speed of deployment that Kasada provides. 'You can be up and running in minutes. Kasada has nailed the onboarding process and once you start to see bots being blocked in real time, wanting to turn it off becomes really hard – they've nailed the customer acquisition fierce.'

The company's latest success includes securing a $7 million investment led by CSIRO's venture capital fund Main Sequence Ventures, Westpac's venture capital fund Reinventure Group, and In-Q-Tel, the internationally respected non-profit organisation that delivers technology capabilities to support the Australian and US national security communities.

Kasada will use the capital to hire more Australian-based software engineers, expand its US team, and step up marketing and sales support. In the past 12 months, the company has doubled its team and revenue, and rolled out more bot fighting technologies.

'In today's highly connected world, a secure digital experience is key to building and retaining trust,' says Crowther. 'Smart businesses know cyber security, data protection and customer experience are inextricably linked.'

3 THE CHALLENGE: AUSTRALIA NEEDS TO PLUG THE WORKFORCE GAP, REMOVE STARTUP BARRIERS, STRENGTHEN R&D, AND MEASURE GROWTH AND IMPACT

> "
> Despite the recent growth in Australia's core cyber workforce, a substantial number of positions remain unfilled because companies can't find the right talents

3.1 OVERVIEW

Four major challenges are detracting from the growth outlook for Australia's cyber security sector:

- A shortage of job-ready workers

- A lack of focus in research and commercialisation

- Barriers to growth and export for smaller local cyber security providers

- A lack of robust measurement of the sector's development and economic impact.

The severe shortage of job-ready cyber security workers is a key challenge. It is estimated that Australia may need around 16,600 additional cyber security workers for technical as well as non-technical positions by 2026.

But despite the recent growth in Australia's core cyber workforce, a substantial number of vacant cyber security positions remain unfilled because companies can't find the right talents. In a promising sign, the education system has begun to mobilise, with a large number of universities and TAFE colleges launching new cyber security degrees and courses. However, it will take time before this pipeline of graduates is ready to enter the workforce, and even then they may face obstacles because of outdated hiring practices.

In the meantime, Australia's cyber security sector will need to draw heavily on workers with transferrable skills from other industries, such as the broader IT sector. There are signs that companies could offer stronger training pathways to accelerate the transition of workers from outside the sector into cyber security roles. The section *Make Australia the leading centre for cyber security education* in Chapter 4 outlines the most promising ways to address these bottlenecks, including stronger partnerships between training institutions and businesses.

Strong research and development (R&D) is the backbone of a thriving cyber security sector. Customers in cyber security, more than in other industries, rely on technological innovation to effectively protect their digital assets from adversaries. Australia's public spending on cyber security R&D and efforts to foster research collaborations between universities and businesses – viewed as crucial for a vibrant, innovation-driven industry – lack focus and lag other leading cyber nations such as the US and Israel. There are also signs that Australian cyber security startups face greater difficulty to commercialise innovative ideas than their global peers, due to a lack of early-stage venture capital.

3 THE CHALLENGE: AUSTRALIA NEEDS TO PLUG THE WORKFORCE GAP, REMOVE STARTUP BARRIERS, STRENGTHEN R&D, AND MEASURE GROWTH AND IMPACT

The section *Growing an Australian cyber security ecosystem* in Chapter 4 offers some solutions to overcome this challenge, including concentrating Australia's cyber security research efforts on a small number of topics that match existing strengths and support the three focus segments.

The third challenge is overcoming market barriers that hamper local companies in their efforts to scale their operations and become leading exporters. Many startups lack a clear understanding of customer needs. Many also lack the credibility to win government agencies or large private businesses as anchor customers. GovPitch, an initiative by AustCyber launched in 2017, is removing some hurdles for small companies to become government contractors. However, complex procurement processes in the public and private sector may prevent smaller companies from scaling their operations. The section *Exporting Australia's cyber security to the world* in Chapter 4 outlines a range of strategies to tackle these issues, such as relaxing current procurement procedures.

Measuring the cyber security sector is emerging as another important challenge to its continuing development. Despite the growing recognition that cyber security is an essential pillar of the modern economy, there is a significant gap in our understanding of the size and development of the sector, as well as its impacts across the economy at large. This blindspot is due to the twin challenges of poor-quality data and the analytical difficulty of measuring cyber security capabilities embedded within many organisations across all sectors of the economy, in addition to those firms in the 'vertical' cyber security sector itself. The section *Provide robust measurement of the sector's development and impact on the Australian economy* in Chapter 4 outlines some actions to tackle these issues over the short and long term, such as launching a measurement program that is both credible and easily repeatable.

3.2 SKILLS AND WORKFORCE GAP

Strong cyber security skills and capabilities are a key driver of economic activity across the Australian economy and are critical for Australia's future prosperity.

'Cyber literacy', or knowing how to effectively protect digital assets, is not only relevant for professionals working in the cyber security sector, it is also becoming a must-have skill for every Australian worker in the digital age, regardless of occupation. All Australian organisations that rely on the internet to conduct business today need a 'cyber-literate' workforce that can secure it against routine cyber risks. A robust education in cyber literacy is a foundation for workplace security, and several national initiatives are already helping to raise the cyber literacy of the broader workforce.

This Sector Competitiveness Plan focuses on the specialised professionals working in the cyber security sector. In Australia, this core cyber security workforce continues to grow. However, current growth is insufficient to cover the rapidly increasing demand for cyber security specialists.

Analysis undertaken for AustCyber's inaugural Sector Competitiveness Plan in 2017 indicated that Australia is facing a severe shortage in specialised cyber security workers.[1]

New analysis for this updated 2019 plan reveals that the cyber security skills gap is larger than initially anticipated and is costing both the sector and the broader economy

New education programs are critical for filling the skills gap in the long-term. Over the past year, universities and vocational training providers have accelerated efforts to launch new cyber security courses and degrees. Partnerships with employers are helping to improve the quality of cyber security education by focusing curricula more on industry needs and facilitating more on-the-job training opportunities.

However, the cyber security skills shortage in Australia will remain severe in the medium-term unless employers start offering better pathways for workers to transition from other industries into cyber security roles. Most workers currently taking up roles in the Australian cyber security sector have previously worked in

---

1   In this plan, the skills shortage is defined as the additional number of workers that would be in the core cyber workforce if the supply of suitable workers was unconstrained. Given the difficulty of modelling an unconstrained sector, other sectors that are less constrained than cyber, such as IT generally, are used as benchmarks.

broadly similar roles in IT and other industries. But to develop strong cyber defences, Australia needs to build a more diverse workforce with both technical and non-technical skills. Improving the gender balance will also help the cyber security workforce grow and mature.

The Australian cyber security workforce is growing, but skills shortage still severe

Every workplace requires a cyber-literate workforce. All-employees, including managers and board members, need a basic ability to implement cyber hygiene in the workplace (daily practices and routines to keep online information secure), as seen in Figure 17. Ensuring every Australian worker acquires basic cyber literacy is fundamental to securing Australian workplaces, large and small, from malicious cyber activity.

Public health provides an analogy. A healthy population has a balanced diet, exercises regularly and minimises risky behaviour like smoking and excessive consumption of alcohol. Similarly, in a cyber-literate workforce all workers use strong passwords, can identify suspicious online activity such as phishing emails, and minimise risky online behaviour, including oversharing personal information or using public WIFI without Virtual Private Network (VPN) protection or other adequate defences.

Several national initiatives have been launched to help equip every Australian with the cyber literacy required to thrive in the digital age. This includes programs aimed at improving company directors' understanding of cyber security.[2]

The Australian Industry and Skills Committee is currently reviewing the cyber skills workers will need in the future, to develop new common training units across multiple industry approved training packages.[3] The intention is to ensure all people skilling or re-skilling through vocational education and training in Australia, regardless of their field of study, will acquire at least a basic competency in cyber security.

Still, at times even the most cyber-literate workers will require expert help from specialised cyber security professionals. Just like the medical profession has different specialists for different ailments, Australia's core cyber security workforce now consists of a range of specialists.

Many organisations in Australia have begun to build designated teams with specific cyber security knowledge, skills and abilities. These are mostly larger organisations, including big banks, with an in-house requirement for workers with a dominant function and role in cyber security. They are typically lead by a CISO. Organisations may also outsource their cyber security needs and contract cyber security professionals from external specialist providers, such as software or services companies.

Cyber security skills are therefore essential for both:

- a general cyber-literate but non-specialist workforce
- a specialised workforce with technical and non-technical professional cyber security skills (see Figure 17).[4]

Figure 17

Cyber skill needs in a typical Australian workplace

Board or governance committee	
CEO and senior management	CISO/CSO
Broader workforce	Cyber security job roles

Non-specialist: Cyber literate employees requiring general cyber hygiene skills

Specialist: Employees with a job role specifically related to an organisation's cyber security across different functional areas. Based on NICE Framework

2   See for example Australian Government (2017), *Australia's Cyber Security Strategy.* First annual update. Available at: **https://cybersecuritystrategy.pmc.gov.au/first-annual-update/a-cyber-smart-nation.html**.

3   More information available at: **https://www.skillsforaustralia.com/cross-sector-projects/cyber-security/**.

4   Analysis in this Sector Competitiveness Plan focuses on the specialist, or core, cyber security workforce in Australia.

Growth is not sufficient to meet demand

Latest data indicates that Australia's core cyber security workforce is growing strongly, but not sufficiently to fill the substantial short-term demand for cyber security professionals.

Australia's core cyber workforce has increased 13 per cent to around 20,500 workers over the past three years (see Figure 18). While government, industry and educational institutions have all undertaken a range of initiatives to strengthen workforce growth

(see Chapter 4 for details), the inevitable delay in any skills system means that the impact of these efforts is yet to be fully realised. Workforce growth has been driven by workers transitioning from adjacent sectors such as IT. Graduates and skilled migration – the two other key sources of supply – have so far contributed relatively little to Australia's cyber security workforce growth.

Figure 18

Cyber security workforce

Australia's cyber security workforce size

# of cyber security workers, 2015–2018
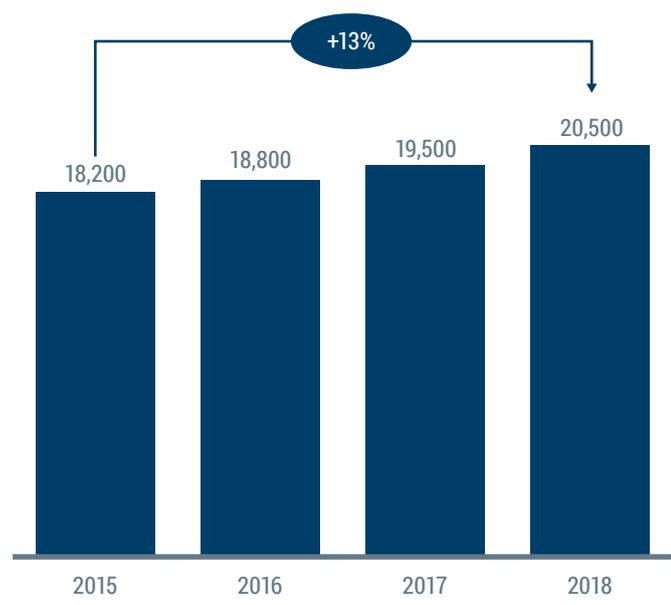
Cyber security workforce composition by NICE categories

% of total cyber security workforce, 2017
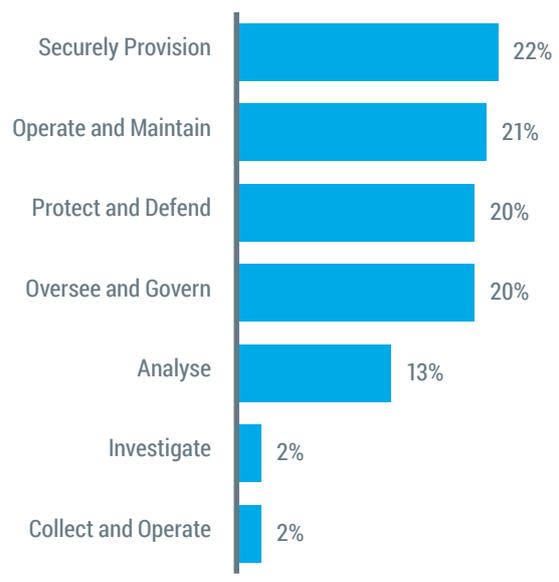
Note: Distribution of cyber security workers across NICE categories derived using the distribution of job ads across NICE categories for 2017
Source: Gartner; TalentNeuron; AlphaBeta Analysis

5   At present there are only around 150 ICT Security Specialists in Australia on Temporary Resident (Skilled) visas (becoming Temporary Skill Shortage visas). While there are likely to be other ICT professions working within the cyber security sector, the total number is unlikely to be more than 200 workers, or around 1 per cent of the core cyber workforce. See: Department of Home Affairs (2018), 'Temporary resident (skilled) visa holders in Australia at 31 December 2017'. Available at: https://data.gov.au/dataset/visa-temporary-work-skilled/resource/995ce658-a956-485a-a593-b3d50407fd93.

Most workers based in the eastern states

Australia's core cyber security workforce is concentrated in the eastern states, with New South Wales hosting the largest number of cyber security professionals, closely followed by Victoria (see Figure 19) then Queensland. The Australian Capital Territory (ACT), though small in population, has experienced the fastest growth in the cyber security workforce. Between 2015 and early 2018, the ACT's core cyber security workforce increased by more than 60 per cent. This is likely a consequence of the Government's focus on strengthening the cyber defence capabilities of government agencies. The workforce growth is set to continue as the Australian Defence Force (ADF) and other departments continue to expand their cyber teams.[6]

Roles becoming increasingly diverse

As employers adapt their business practices to the digital economy, their requirements for an increasingly diverse range of cyber security specialists has become more apparent. It is no longer useful to think of the cyber security occupation as one uniform job role or skill set.

Today, cyber security comprises a range of technical roles from architecture to operations and newer, multidisciplinary, non-technical roles that incorporate elements of law, risk, communications and psychology.

While the face of the cyber security workforce is changing fast, Australia has not yet adopted a widely accepted skills framework to describe the various cyber security work roles

Other countries have already taken action. For example, the US National Initiative for Cybersecurity Education (NICE) has developed a Workforce Framework to standardise the taxonomy of cyber security occupations (see Box 8). It is a comprehensive, skills-based categorisation of cyber security roles. Companies in the US and other countries are using the framework as a common nomenclature for identifying the skills required in the cyber security workforce.

Figure 19

Australia's cyber security workforce by state

\# of cyber security workers, 2017

NT
<500

QLD
~3,000

WA
~1,500

SA
~1,000

NSW
~7,000

ACT
<1,000

VIC
~5,500

TAS
<500
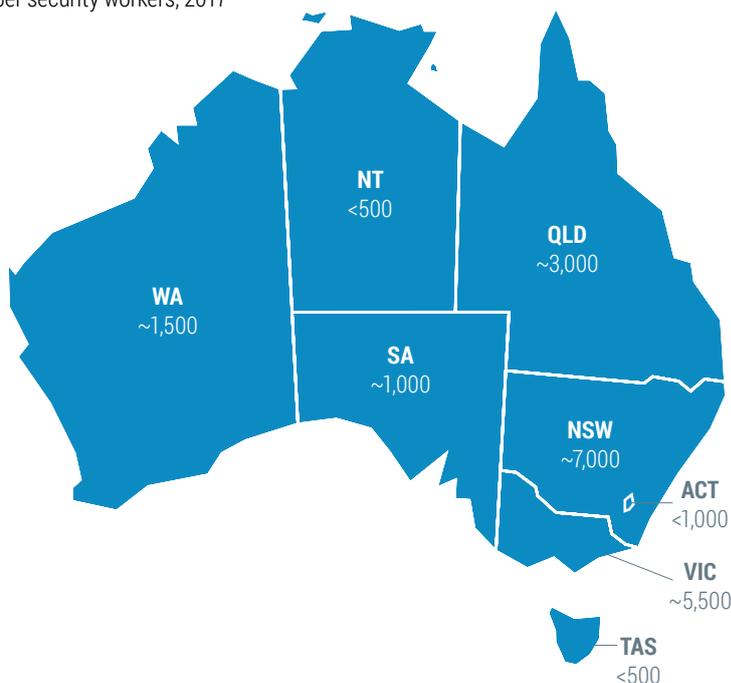
Note: Distribution of cyber security workers across States derived from distribution of most relevant cyber ANZSCO occupations in ABS Cat 6291.
SOURCE: Gartner; AlphaBeta Analysis

---

6   The ADF announced the establishment of an Information Warfare Division in July 2017. Further information available at: **www.defence.gov.au/jcg/iwd.asp**.
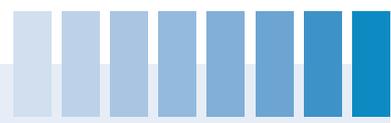
Box 8

NICE: A standardised framework to understand what cyber security professionals do

The US National Initiative of Cyber Security Education (NICE), led by the US Department of Commerce, is a partnership between government, academia and the private sector that seeks to improve the America's cyber security education, training, and professional development.[7] The NICE program could serve as an example for Australia, which has yet to implement a comprehensive set of definitions to classify its cyber security workforce.

A critical part of the NICE program is a standardisation of cyber security roles, based on the skills, knowledge and tasks needed to perform them. By providing such a framework of professional role categories, NICE closes a crucial information gap at a time of a global shortage in cyber security skills. For example, many cyber security roles have not yet been well defined or understood, there is a lack of consistency among cyber training programs, and many potential employees don't know which skills are required in different cyber security jobs.

The NICE Workforce Framework consists of seven categories of cyber security work:

| Categories	Description
Securely Provision	Designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development
Operate and Maintain	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security
Oversee and Govern	Provides leadership, management, direction, or development and advocacy so the organisation may effectively conduct cybersecurity work
Protect and Defend	Identifies, analyses, and mitigates threats to internal information technology (IT) systems and/or networks
Analyse	Performs highly-specialised review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence
Collect and Operate	Provides specialised denial and deception operations and collection of cybersecurity information that may be used to develop intelligence
Investigate	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence

These categories are further divided into 32 specialty areas, 52 work roles and hundreds of tasks, skills, knowledge and abilities.

The NICE Framework enables organisations to identify their cyber security skill needs and assess the aptitude of their existing cyber security workforce. It can also be used to inform hiring practices and offers a common terminology to effectively communicate cyber security needs both internally and with stakeholders. In addition, education and training institutions can use the NICE framework to align their curricula with an accepted standard of cyber security knowledge, skills and abilities.

The NICE Framework is updated regularly to ensure it remains relevant as the nature of the cyber security workforce changes. Education providers and employers, both in the public and private sector, provide key information for the updates, allowing the Framework to continuously serve as a fundamental reference.

---

7   National Initiative for Cybersecurity Education (NICE). NICE Cybersecurity Workforce Framework.
     More information: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework.

Structure of NICE Workforce Framework

7 Categories

32 Specialty Areas

52 Work Roles

Tasks, knowledge, skills and abilities
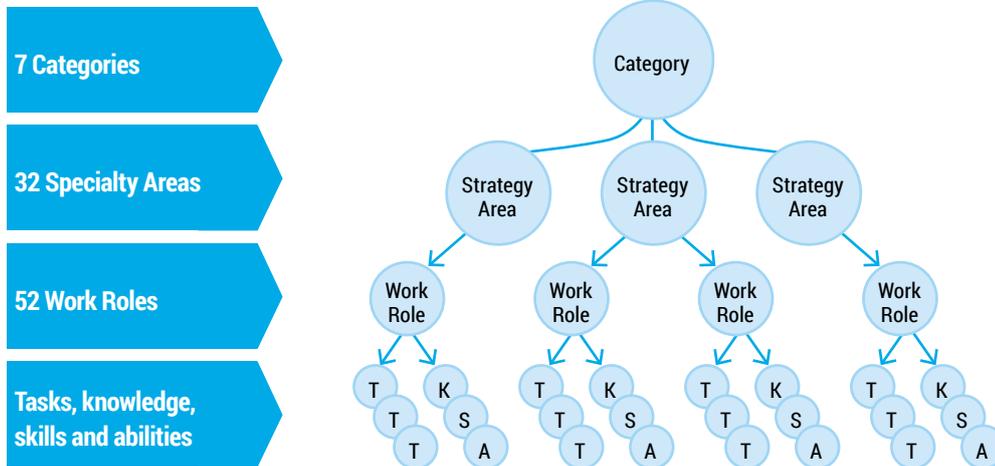
SOURCE: Nice Framework

For Australia, the NICE Framework offers a template to understand the skill needs of its cyber security workforce. This is particularly important for policymakers and company executives who are looking for ways to overcome the current skills shortage.

Using the NICE Framework, the makeup of the cyber security workforce can be explored in detail. As shown in Figure 18, most cyber security workers in Australia currently work in roles related to building, buying and operating secure IT systems (Securely Provision, Operate and Maintain, Protect and Defend). Meanwhile, workers tasked with cyber-related intelligence and law enforcement activities (Collect and Operate and Investigate) are occupying a niche. Overall, the composition of the Australian cyber workforce is broadly comparable with the US workforce, though with a greater emphasis on identification and mitigation of threats, and leadership and management of cyber security (Protect and Defend and Oversee and Govern).

There is a tendency to think that the cyber security workforce consists only of highly technical professionals. However, today's cyber security workforce encompasses a variety of roles and responsibilities that require non-technical skills and abilities. For example, the Oversee and Govern category includes legal advice, cybersecurity management, strategic planning and policy, training education and awareness, and change management. Employers report in interviews that 'soft skills', including the ability to work in teams across an organisation and to communicate clearly (both verbally and in writing), are important across almost all cyber roles, and are often in short supply. These skills ensure that the cyber function within an organisation is able to effectively engage across other parts of the organisation and implement processes and practices that recognise and respond to the human dimension of cyber security.

Employers have also noted in interviews that cyber defences are most effective if an organisation employs a diverse team of cyber security specialists – people with different backgrounds and viewpoints, and a wide range of skills. Building real workplace diversity goes beyond pure skills. It also requires a balance of cultures and gender among staff.

'We need people from more diverse backgrounds, a diversity of thought is essential for our cyber defences us.'
Cyber security manager of an ASX 100 company

Despite this acknowledgement, the gender diversity in the Australian cyber security sector remains weak. The share of women working as ICT Security Specialists has declined from 22 per cent to 19 per cent over the 10 years to 2016, according to the Australian Census of Population and Housing.[8] Australia appears to perform better on this measure than global peers, with evidence suggesting only 14 per cent of cyber security professionals in North America and seven per cent in Europe are female.[9] However, much more has to be done to improve the gender balance in Australia's cyber security sector.

8   ABS (2018), *Australian Census Longitudinal Dataset*.
9   Nature (2018), 'Cybersecurity needs women'. Available at: **https://www.nature.com/articles/d41586-018-03327-w**.

Job market indicators show employers are struggling to fill cyber security roles

The first version of this Sector Competitiveness Plan, published in 2017, noted that Australia's cyber security sector is grappling with a substantial skills shortage – an assessment that relied largely on anecdotal and survey evidence. For example, in 2016, three out of four local cyber security professionals surveyed by the Australian Information Security Association (AISA) said their industry is facing a severe skills shortage, as shown in Figure 20. A similar survey, undertaken by the Centre for Strategic & International Studies (CSIS) and Intel Security across eight countries, paints an even more concerning picture. It reveals that the talent drought affecting the Australian cyber security sector is one of the worst in the world: 88 per cent of Australian cyber security professionals observe a skills shortage in their industry. Extensive interviews with cyber security users and providers in Australia support the survey results.

> "The talent drought affecting the Australian cyber security sector is perceived to be one of the worst in the world

Figure 20

AISA survey (2016)

Australian professionals report a skills shortage*

Share of responses to the question 'Is there a cyber security skills shortage in Australia?'

No 9.0%
Don't know 14.0%
78.0% Yes

CSIS survey (2016)

Australia has the worst perceived skills shortage out of the countries surveyed†

% of industry participants reporting a shortage of cyber security professionals in their country

Country	%
Australia	88
Mexico	88
Japan	84
Germany	83
US	83
Israel	80
France	75
UK	75

* Based on a survey of 241 AISA members (consisting of Australian cyber security professionals)

† Based on a survey of 775 cyber security professionals from 8 countries (including 75 from Australia)

SOURCE: AISA (2016) The Australian Cyber Security Skills Shortage Study; CSIS (2016) 'Hacking the Skills Shortage'

Skills shortage more severe than expected

This updated Sector Competitiveness Plan provides further insight into the workforce, with an estimate of the severity of Australia's cyber skills shortage. New research, undertaken exclusively for this plan update, draws on a range of job market data to show that the skills shortage in Australia's cyber security sector is more severe than expected and is already creating real economic costs.

Despite the recent growth in Australia's core cyber workforce, companies have been struggling to fill a substantial number of vacant cyber security positions. Figure 21 aggregates data across wages, recruitment failure rates, the time to fill a position, and the size of the potential candidate pool (job market depth). All indicators strongly point to a substantial skills shortage in the Australian cyber security sector.

Wage premium: Wages are high across the cyber security profession with a $12,000 average wage premium paid for a cyber security worker over an IT worker. Cyber security workers in all but one NICE category (Operate and Maintain) earn more on average than the average IT salary. Roles in management and leadership, and involving design and build of cyber systems, are currently commanding the highest salaries, with average wage premiums of more than $20,000 above general IT. This may partly reflect more acute shortages, but also the level of experience and specialisation required to perform these roles.

> *'We are offering workers $100k plus, who are getting their first job in cyber.'*
> CISO, large Australian company

Recruitment failure rate: Labour market research on IT professions from the Australian Department of Jobs and Small Business shows that 42 per cent of ICT Security Specialist vacancies in Australia went unfilled in 2015 – significantly more than the average recruitment failure rate of 33 per cent across the broader IT sector.[10] The research also found there were on average only 1.7 suitable applicants per vacancy for ICT Security Specialists, which was the lowest number across all IT professions studied.

Recruitment time: Recruitment difficulties appear widespread in the cyber sector. Interviews with industry participants suggest it takes 20 to 30 per cent longer to fill a cyber security role compared with roles in the IT sector.

> *'We can find the right people, but it can take much longer than for other jobs, it can take two or three months of searching.'*
> Cyber security manager, large Australian company

Job market depth: Job market depth is defined as the number of people employed in an industry per job ad, which is used as a proxy measure for worker supply. The job market for cyber security has less depth than either IT or the broader economy, with less than seven people employed in the sector for every job ad.

Any of these job market indicators, when looked at in isolation, would not provide conclusive evidence that Australia's cyber security sector is facing a skills shortage. However, the fact that all four indicators point in the same direction – significantly tighter conditions than either the wider IT sector or the workforce as a whole – clearly demonstrates that cyber security is facing major labour market constraints.

---

10   Department of Jobs and Small Business (2015), *Labour Market Research – Information Technology (IT) Professions, December Quarter 2015.*

Figure 21

Skills shortage indicators in cyber security

1 Wage premium

Salaries, AUD, 2017
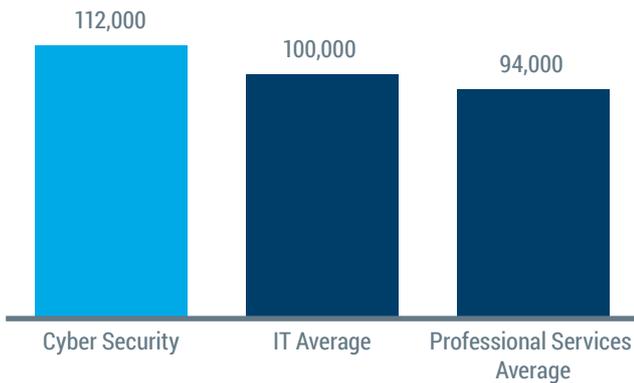
SOURCE: ABS

2 Recruitment failure rate

% vacancies unfilled, 2015
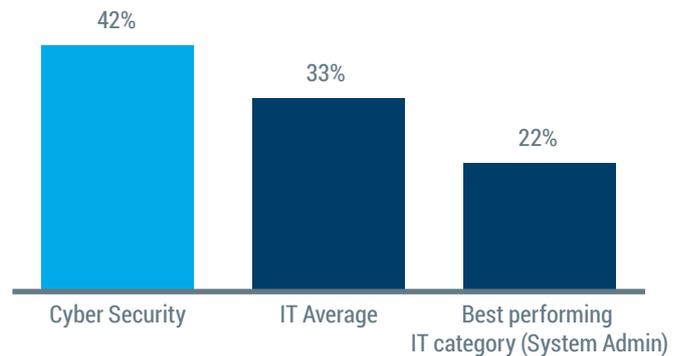
Note: Cyber security rate implied from ANZSCO class *ICT Security Specialist*
SOURCE: Dept. of Jobs

3 Recruitment time

Time to fill, 2017
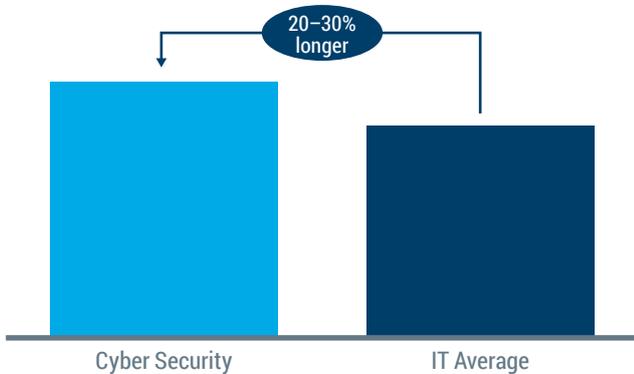
SOURCE: TalentNeuron, industry interviews

4 Job market depth
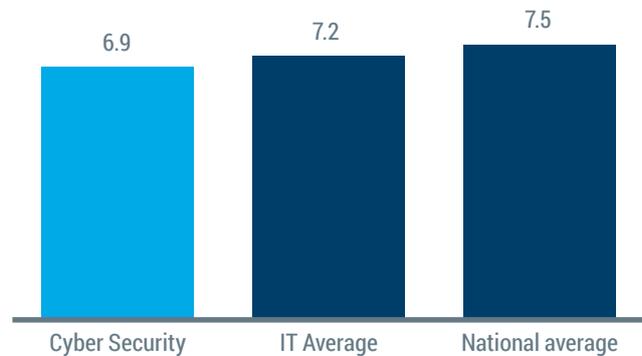
SOURCE: TalentNeuron, ABS, Deloitte Digital Pulse

The skills shortage is costing the sector and the wider economy

Measuring the precise size of a skills shortage is difficult because of the dynamic nature of labour markets. Calculations using a range of methodologies, based on a combination of the job market indicators described above, suggest Australia's cyber security sector was short 800 to 2,300 workers in 2017. That is equivalent to roughly 4 to 12 per cent of the total Australian cyber workforce in that year (see Figure 22).[11] This is likely to be a conservative estimate because it is based on only observable labour market behaviour and does not account for depressed growth expectations as a result of the perception of the shortage. In other words, employers know it will be difficult to find cyber workers at wages they can afford, so they never create or advertise positions they might like to fill.

The workforce shortfall has significant economic consequences. The cyber security sector is estimated to have forfeited up to $405 million in revenue and wages in 2017, which it could have generated if companies had been able to find the cyber security workers to fill existing vacancies.

The cyber security sector is estimated to have forfeited up to $405 million in revenue and wages in 2017

This loss of revenue and wages only represents the direct cost to the cyber sector. The cost to the wider economy is likely many times greater because the skills shortage in the cyber security sector has a ripple effect throughout the economy that would propel the true economic cost far higher. As the cyber sector is a critical enabler of broader economic activity, workforce constraints can curtail revenue growth in the wider economy. For example, a lack of security staff could make an organisation more prone to cyber attacks, which would undermine business and consumer confidence and lower the productivity of workers because of service downtime. It is difficult to accurately estimate the indirect economic costs of the skills shortage due to limited data on the economic benefits of cyber investments and, conversely, the consequences of cyber breaches (see *Size of the prize* in Chapter 2 for further discussion). However, anecdotal evidence suggests the shortage of cyber skills is already causing organisations to slow their digital transformations.

Figure 22

Estimated cyber security workforce supply shortage

workers, 2017
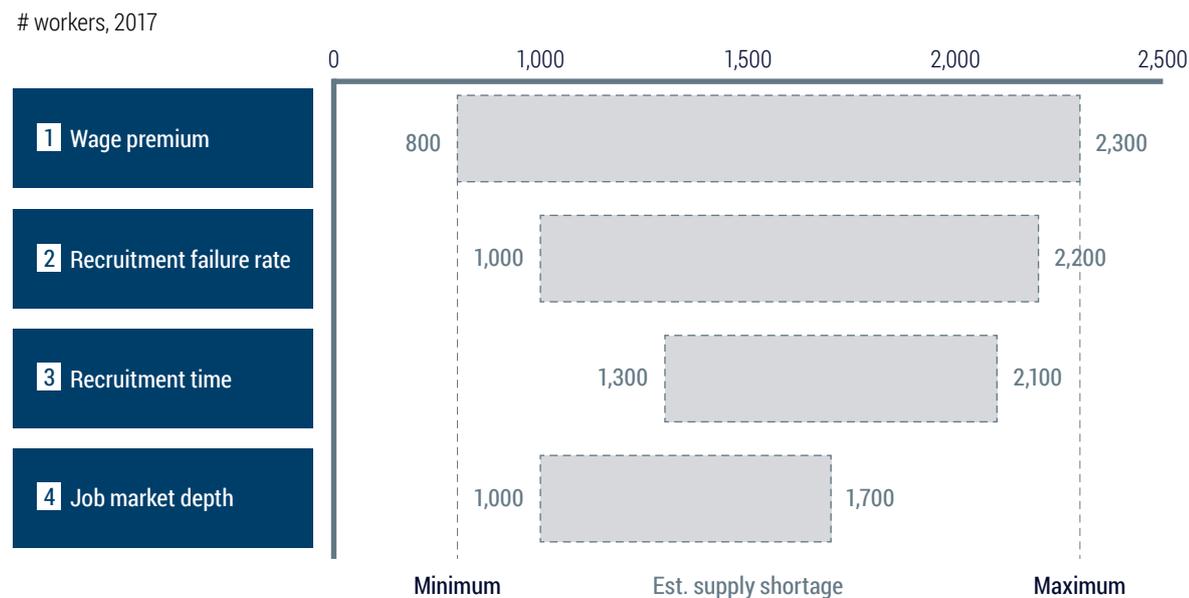
SOURCE: Gartner, TN, ABS, AlphaBeta Analysis

---

11   The estimate was generated using the four different job market metrics. See Appendix B for details.

## Lack of skilled workers is not the only cause of the skills shortage

The apparent lack of skilled workers is not surprising given cyber is a young and emerging profession that has faced rapid demand growth and limited educational pathways. It is also a product of the increased need for cyber security experts and broader cyber security awareness and literacy among all workers in a period of rapid digitisation in a fast-moving technological landscape.

In addition, there are signs that employers' hiring practices may be exacerbating the lack of skilled workers. For instance, two-thirds of information and cyber security professionals surveyed by the Australian Information Security Association in 2016 cited management's failure to understand skills requirements as a key driver of the current cyber skills shortage, while just over half said employers were reluctant to recruit and train entry-level candidates for cyber security roles.[12]

'HR writes position descriptions based on things that they know how to assess, like qualifications and experience. The new cyber security workforce doesn't yet have these qualifications or experience.'
CISO, large Australian company

An analysis of cyber security job ads supports the survey findings. As shown in Figure 23, employers advertising cyber roles tend to demand more work experience from cyber security professionals compared with other workers in the broader IT and professional services sector. On average, one-third of cyber security job ads request more than eight years of experience. In some roles (for example, in the NICE Collect and Operate category), almost half (49 per cent) of all job ads demand such extensive experience.

Figure 23

Breakdown of job ads by experience requested

% of job ads, 2017   ■ 0–2 years experience   ■ 3–7 years experience   ■ 8+ years experience

	Professional Services	IT	Cyber Security	Securely Provision	Operate and Maintain	Oversee and Govern	Protect and Defend	Analyse	Collect and Operate	Investigate
Total	100	100	100	100	100	100	100	100	100	100
8+ years	23	30	33	31	25	40	36	32	49	30
3–7 years	55	54	54	56	59	51	54	52	37	49
0–2 years	22	16	13	13	16	9	10	16	15	22

SOURCE: TalentNeuron; AlphaBeta Analysis

12   Australian Information Security Association (2016), The Australian Cyber Security Skills Shortage Study 2016. Available at: https://www.aisa.org.au/CyberSkillsReport.

With continued strong demand forecast, the shortage is likely to persist

Demand for cyber security workers is set to remain strong in coming years, meaning the skills shortage will not ease without consistent efforts to increase supply. As shown in Figure 24, the sector could require up to 16,600 additional workers by 2026.

This estimate is made up of several components:

- The first Sector Competitiveness Plan in 2017 identified an additional 11,000 workers would be needed by 2026 just to meet the current growth of cyber security needs in Australia (business-as-usual demand). There has been some progress over the past 2 years, with around 1,700 workers added to the sector.

- However, the current skills shortage of up to 2,300 cyber security workers still needs to be filled.

- Up to 5,000 more workers could be required if the cyber sector significantly lifted its performance in three key areas identified in Chapter 2.

> Australia's cyber security sector could require up to **16,600** additional workers by 2026

Figure 24

Forecast additional cyber security workers in 2026

Number of workers

~11,000	1,700	800–2,300	~5,000	~16,600
Baseline BAU estimate	Progress since 2017 SCP	Filling current supply shortfall	Uplift from strong industry performance	High range estimate

Around 1,700 workers are estimated to have joined the cyber security workforce over the last year
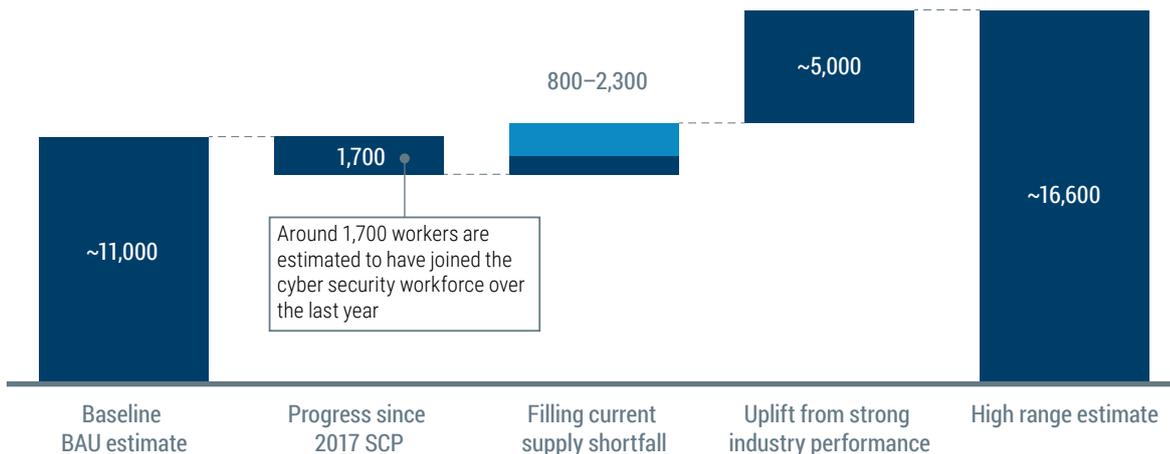
SOURCE: Gartner, ABS 2011 Census, ABS (2016) '3401.0 – Overseas Arrivals and Departures', ABS (2016) '6202.0 – Labour Force', stakeholder interviews, AlphaBeta and McKinsey analysis

3 THE CHALLENGE: AUSTRALIA NEEDS TO PLUG THE WORKFORCE GAP, REMOVE STARTUP BARRIERS, STRENGTHEN R&D, AND MEASURE GROWTH AND IMPACT

Australia's education system is mobilising, but faces risks

Education and training providers play an important role in supporting the expansion of Australia's cyber security sector. Companies will only be able to draw on new cyber security talent if TAFEs and universities offer a wide variety of cyber security qualifications that are attractive to students and relevant to employer needs. Encouragingly, the education system has begun to mobilise over the past several years. A significant number of TAFEs and universities are now offering courses or degrees in cyber security.

However, there are risks to this mobilisation that Australia needs to address.

- **Student demand** will need to grow strongly to fill the new courses being created. Improving the cyber security talent pipeline needs to start in primary and secondary schools. The more schools encourage students to consider a career in cyber security, and the more they foster early skills, the higher the quality of students in the tertiary education system will be. This means schools should place greater emphasis on developing cyber security skills in curricular and extracurricular programs as pathways to higher education.

- High schools and tertiary education providers must find ways to encourage more **female students** to pursue cyber security related programs to help improve gender diversity in the industry.

- **Shortages of teaching staff** are affecting universities and TAFEs.

- There is **lack of funding** for the required technical infrastructure, like cyber ranges (virtual or physical spaces for simulating real-world scenarios) and cyber labs, to train the next generation of cyber security workers.

- Rapid growth in educational programs poses a risk to **course quality**. Yet high-quality education that matches industry needs is essential to ensure graduates acquire the right skills to find a job.

Universities and TAFEs are launching new cyber-specific courses

TAFEs and universities around the country have rapidly expanded their cyber security program offering in recent years, often in close partnership with industry. Approximately half of all universities in Australia are now offering cyber security as a specific degree or as a major in IT or computer science university qualifications. Another quarter offer at least some cyber security course units. As of March 2018, only 20 per cent of Australian universities do not yet offer any cyber security units or courses. This led total enrolments and completions in university courses classified as security science to almost double between 2012 and 2016.[13]

Approximately half of Australia's universities now offer cyber security as a specific degree or a major in IT or computer science qualifications

Multidisciplinary cyber courses are becoming increasingly common in Australia. The University of Western Sydney now offers a Bachelor in Cyber Security and Behaviour, which focuses on the human and technical sides of cybercrime and includes a number of units in psychology. The University of New South Wales Canberra now offers a Master in Cyber Security, Strategy and Diplomacy in the School of Humanities and Social Sciences. This interdisciplinary course focuses on the interplay between cyber security, strategy and diplomacy. Latest course trends reflect the evolution of cyber security education outside its traditional home in ICT faculties and departments as well as the growing demand from employers for graduates with strong policy writing, risk management and strategy skills to work in cyber security related roles in their organisations.

The vocational education and training sector is also increasing the emphasis on cyber security education. Leading TAFEs around the country joined forces in late 2017, coordinated nationally by AustCyber, to play a greater role in providing nationally consistent cyber security training. Box Hill Institute in Victoria has been paving the way with the development of two new cyber security certificate and diploma-level courses that are now being taught across the country. These offerings help to diversify the range of education pathways into the cyber security sector and provide a high-quality vocational cyber security training option that is in high demand by Australian employers.

---

13   Department of Education and Training (2018), *Higher Education Statistics.* In 2016, there were 1,150 enrolments and 231 completions from security science courses. While security science is the only cyber-specific field of education, some cyber security courses or other courses with significant cyber components are likely classified elsewhere and not captured in these totals. Student numbers for 2017 and 2018 are not yet available.

Together, the new cyber-specific degrees and courses will have a strong positive impact on Australia's future cyber security workforce supply. It is expected that even without the addition of further courses or new institutions teaching cyber, current plans could see the number of cyber graduates increase from around 500 per year in 2017 to about 2,000 a year in 2026. Assuming the quality of graduates remains strong, this growth will make a significant contribution to closing the skills shortage and meeting employer demand for cyber security workers in the long-term.
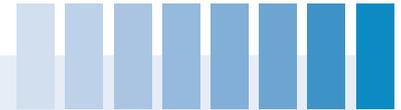
Box 9

Industry collaboration sets the standard for interactive cyber security education

Educating and training the cyber security workforce of today and tomorrow has become a critical industry that is under constant pressure to fill vacant positions with skilled staff at all levels.

This, coupled with the lack of formal education pathways, led Canberra-based startup Fifth Domain to seek funding from AustCyber to address the gap in specialist cyber security training and education solutions.

Fifth Domain was awarded a project to the value of A$1 million through AustCyber's Projects Fund to produce a learning management system in partnership with the Canberra Institute of Technology (CIT), the Australian National University (ANU) and Nova Systems.

The Certificate IV in Cyber Security, offered by CIT as part of the national TAFEcyber set of industry led qualifications, provided the framework for a Training Security Operations Centre (TSOC), with content delivered through Fifth Domain's Learning Labs. The learning outcomes were then mapped at CIT and ANU to the job roles provided under the internationally recognised US National Initiative for Education's Workforce Framework – providing students with visibility of their skills, and a clear learning pathway and potential career options.

The success of the project means Fifth Domain can develop and deliver standardised training materials for all Australian TAFEs and universities, equipping students with consistent skills critical to the cyber security workforce.

The project has delivered a number of benefits to the broader Australian cyber security sector. The most significant is the ability to assess skills requirements through a common skills framework to better define workforce requirements. Courses mapped to specific work roles ensures those wanting to begin a career in cyber security are better informed about potential learning pathways.

Importantly, the project has also encouraged CIT and ANU to develop strong working relationships with the local cyber security industry.

Consequently, this project was awarded the 'Industry Collaboration Award' at the ACT Training Awards, and was then a finalist in the Australian National Training Awards – the first nomination for cyber security education and training.
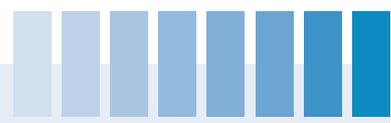
Box 10

SME cyber support creating student jobs

The WA AustCyber Innovation Hub is one of the original partners and supporters of Cyber Check.Me – a partnership between Edith Cowan University (ECU), the Cities of Joondalup and Wanneroo and North Metropolitan TAFE (NMTAFE).

Originally founded in 2012 by Professor Craig Valli and Dr. Ian Martinus to assist small business with their cyber hygiene including passwords, data and device protection, the program has been re-cast and re-launched in 2019 with expanded offerings including compliance with amendments to the Privacy Act and mandatory breach notification.

To date, over 40 students – including many female students from NMTAFE and ECU – have been trained to meet with local businesses, consider their business model and industry segment, and offer basic cyber advice that promotes greater protections and cyber-safeguards. At least six students have created their own businesses specialising in offering practical cyber assistance to SMEs. This number will only grow as more students are interested in setting up their own niche offering.

In 2019, the program extended to workshops in the North West of WA to suppliers in the mining, oil and gas industries in Karratha. Notable flaws included third party verification of vendors and their systems. Similarly, Cyber Check.Me workshops were held in the south west of WA in Bunbury, where students demonstrated the vulnerability of accessing WiFi and unsecure networks to 100 businesses mainly from Agtech backgrounds.

Internationally, presentations to potential export market partners in Indonesia and Malaysia were received with great interest. These relationships will be explored further in 2020.

The program has expanded rapidly in 2019, extending to numerous metropolitan and regional government agencies with access to over 10,000 small businesses. The aim of the program is to strengthen the cyber services ecosystem, where introductory offerings such as Cyber Check.Me can act as a referral to local companies offering higher order service and product offerings.

Risks to the quality and sustainability of cyber education need to be addressed

Despite the push by various education providers to increase cyber security study opportunities, the projections of strong growth in high-quality graduates will not be realisable without addressing a range of risks.

The education system's success in generating a sufficient amount of work-ready cyber security graduates to meet the market demand depends on three key factors:

• student demand for cyber courses

• the sustainability of cyber education

• the quality of the courses in generating job-ready graduates.

Student demand for cyber courses: The number of training places in cyber security education has expanded rapidly and is forecast to continue to grow strongly. To fill these places, student demand also needs to increase significantly and remain of high quality.

A critical barrier complicating efforts by universities and TAFEs to increase the number of skilled graduates is the low level of awareness of cyber security careers among school students. For example, surveys suggest that many Australian secondary students, unlike peers in the UK and the US, are not aware of cyber security careers pathways and job options. Unless this is remedied, post-secondary student demand for cyber security education may not increase fast enough. Tertiary education providers need to ensure cyber security is seen as a desirable study option to attract the best and most motivated students (see Figure 25).

Figure 25

Students noting cyber being mentioned in schooling

Students noting cyber being mentioned in schooling

% of secondary students 2016
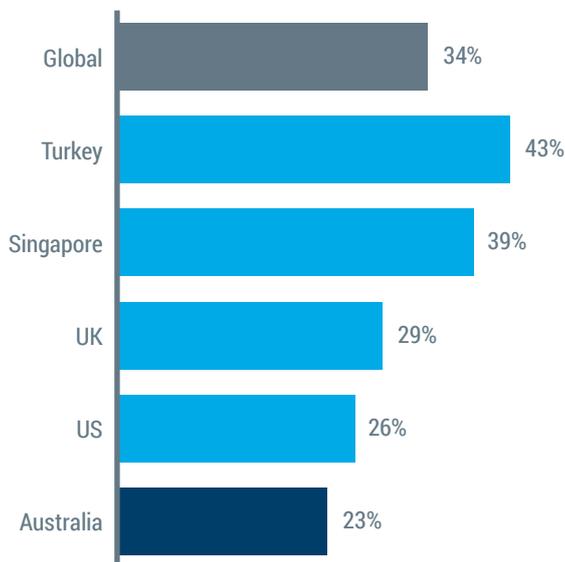
Students who were aware of responsibilities & tasks in cyber profession

% of secondary students 2016
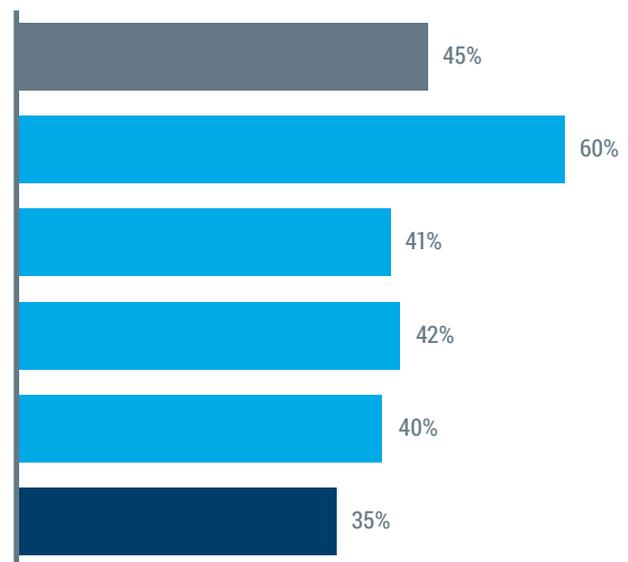
Note: The survey was a study of 3,779 adults aged 18–26 undertaken in 2016 in 12 countries.
SOURCE: Raytheon Australia (2016), 'Securing our future: Closing the Cyber Security Talent Gap', avail. at: www.raytheon.com/cyber/rtnwcm/groups/public/documents/content/aucybersurveysummary.pdf.

Cyber security should be explicitly taught as part of the Digital Technologies component of the National Curriculum. By not doing so, Australia is failing to seize an opportunity to strengthen the cyber security talent pipeline. The next update of the Curriculum is due in 2020. In the meantime, the Curriculum could be enriched by adding cyber-specific learning and teaching resources to the 'Digital Technologies Hub', which supports the Curriculum with practical lesson plans, case studies, advice and activities to be included in relevant classes. An increased focus on cyber security in the National Curriculum will help build interest in cyber careers and will the cyber literacy of all students, which is critical for improving cyber hygiene and understanding in the broader Australian workforce.

Cyber security challenges play an important role in developing and testing practical skills while generating interest in cyber security careers. For example, the 'CyberPatriot' program in the US is a competition where teams of high school students can experience the work day of IT professionals with responsibility for managing the network of a small company. Teams are tasked with identifying cyber security vulnerabilities and increasing the robustness of the system. Successful students earn both national recognition and scholarship money for further studies. The competition has proven to lift the profile and awareness of cyber security careers. Implementing a similar competition in Australian high schools would almost certainly have the same affect.

Implementing more focused cyber security competitions and awareness programs is as vital as improving the gender diversity in the industry. TAFE data shows that female enrolment in the new vocational cyber certificates and diplomas is as low as 9 per cent, and as high as 20 per cent at best. Unless targeted measures encourage more girls to opt for a career in cyber security, the core cyber security workforce will not develop the diversity it needs to ensure quality and relevance. School programs need to explicitly address this gender challenge in their design. Scandinavian research shows that girls, on average, start to lose interest in STEM subjects at the age of seven and most have lost interest by the age of 14. While no comparable research exists for Australia, the study highlights the importance of school education for future career paths.

Sustainability of cyber education: The increase in cyber security courses over the last few years will only be sustainable with sufficient teaching staff and a stable financial model for providers. Most education providers are reporting difficulties in attracting and retaining skilled cyber security teachers, largely because high-quality cyber security teachers are demanding above-average pay. In some cases, salaries for cyber security professionals in teaching roles are more than 45 per cent lower than salaries for other cyber security practitioners (see Figure 26). Education providers will likely continue to compete for skilled cyber security staff, as the number of cyber security teachers required to meet the skills shortage may triple over the next five years.

> *'Salary is a real issue for us. We can't pay anywhere near what industry can pay.'*
> TAFE program manager

Vocational institutions appear particularly limited to pay higher wages because of financial constraints and enterprise agreements. The problem could worsen if wage growth in the cyber security sector remains strong and demand for teaching staff expands as expected.

Universities are also feeling the pressure. They are not only competing with industry, but also with universities around the world, which can often offer higher salaries and more prestige. Some cyber security professionals are also discouraged from teaching in universities because they are not interested in an academic role or lack the aptitude for academic research.

An increased focus on cyber security in the National Curriculum will help build interest in cyber careers

Figure 26

Average salary range in the cyber industry and in cyber education

$, 2018   ■ Low estimate ■ High estimate

Cyber industry (3+ years experience): 120,000 — 135,000
University lecturers and tutors: 81,000 — 120,000
Vocational education teachers*: 65,000 — 100,000

Notes: Average cyber salary derived from job ad data. University and TAFE salaries derived from 2016 ABS salary data for the relevant ANZSCOs, adjusted for wage growth

* TAFE NSW workers can earn at most $113,000 if they are employed at the highest pay band in the 2016 Enterprise Agreement. However there are a fixed number of positions at each grade so promotion/employment at a particular grade requires an open vacancy

SOURCE: TalentNeuron; ABS; AlphaBeta analysis

Some institutions are investigating new ways of online education and synchronous remote teaching (through video-conferencing and online chat) to use their existing teachers most efficiently. However, e-learning may have an adverse effect if students fail to obtain the practical, hands-on skills that employers demand. Partnerships with industry have allowed course providers to draw on guest lecturers to supplement their permanent teachers – for example, cyber security staff from Commonwealth Bank of Australia have been guest lecturers at University of New South Wales – but to date this approach is only operating at a relatively small scale.

Many education providers also struggle to pay the establishment and maintenance costs of launching new cyber security courses and degrees. Cyber security education can involve significant upfront investments in teaching infrastructure, including cyber security labs, cyber security ranges (virtual or physical spaces for simulating real-world scenarios), and specialised computer hardware and software. In most other disciplines, the technical infrastructure required for the practical delivery of programs has built up over a longer period of time. Education institutions

delivering cyber security programs are therefore on the back foot. They need to be able to rapidly deploy and maintain the technical infrastructure required to produce world-class graduates.

'We could train 300 to 500 people, but we cannot afford to pay for all the infrastructure. Government expects that industry will pay for it, but this is not happening.'
Vocational Education and Training manager in cyber security

Course fees are typically not sufficient to cover these large infrastructure costs, particularly in vocational education and training courses. While both New South Wales and Victoria have supported the new nationally consistent Certificate IV in Cyber Security by placing it on their state skills shortage lists, total fees (government subsidy and student payable fee) for that course are around 9 per cent lower than total fees for a comparable Certificate IV in Information Technology.[14]

14   In New South Wales, the full price (including government subsidies) for a Certificate IV in IT is $8,880 while a Certificate IV in Cyber Security is $8,100. In Victoria the full price (including government subsidies) for a Certificate IV in IT is $9,100 while a Certificate IV in Cyber Security is $8,300.

Universities are facing similar challenges but can usually draw on larger financial resources. Several Australian universities have also been able to attract industry support for investments in educational infrastructure. For example, the Commonwealth Bank of Australia's partnership with University of New South Wales has provided funding for a new lab for experimental, hands-on teaching. Edith Cowan University and Melbourne University have also received additional funding for their cyber security education and research through the Australian Government's Academic Centres of Cyber Security Excellence program – a total commitment of $1.9 million over four years. There is a risk that without a more strategic approach to investment in cyber security teaching infrastructure, the hands-on skills development will not meet these needs of employers.

Course quality: The current expansion of cyber security courses in Australia is healthy and necessary. However, maintaining course quality is essential. A flood of new cyber security education providers will heighten the competition for teaching staff, who are already in critically short supply. This poses a considerable risk to the quality of graduates.

Education providers may also struggle to build a curriculum that is responsive to market changes. Cyber security is a fast-evolving industry where technology and industry needs are continuously changing. Courses need to be flexible and responsive to these changes and designed with ongoing input from industry.

At present, there is no accreditation model in Australia designed specifically for cyber security courses. This is in contrast to the US and UK, where governments have established accreditation programs.[15] The Australian Computer Society (ACS) already accredits IT education programs using the ICT Profession Core Body of Knowledge (CBOK). The Academic Centres of Cyber Security Excellence model could play a role similar to accreditation, but to date only two universities have received support under the program and there are no plans for further rounds.

Strong partnerships between education providers and industry have helped to shape curricula that meet employer needs. However, it will be hard to keep industry involved as more education providers enter the market with their own cyber security offerings. Industry, especially large financial companies and telecommunications companies, are likely to concentrate their time and resources on a few high-performing institutions. This will likely leave some education providers struggling to be responsive to the changing needs of industry and technological progress.

Employers are looking for verifiable proof that new hires have the skills required to do the job. A cyber security challenge model can help them identify talented individuals suited to a career in cyber security. Companies around the world, including Barclays, are increasingly running and sponsoring such challenges to identify and recruit the next generation of cyber security professionals.[16] In Australia, CySCA – Cyber Security Challenge Australia, a partnership between government, business and educational institutions – is the preeminent program for TAFE and university students. Cyber Security challenges could be used as part of an accreditation process. They offer employers an opportunity to identify the best performing educational institutions and the best performing students.

Interviews suggest that the quality of cyber security courses can suffer if work-integrated learning opportunities are missing. Work-integrated learning is embedding meaningful industry projects or placements into an academic program of study. It has been shown to improve graduate employment outcomes by developing more job-ready skills. Research for the Office of the Chief Scientist finds that less than half of IT students in Australian universities have an opportunity to do an industry placement.[17] Work-integrated learning is particularly important in the cyber security sector because there is a greater need for employees to think strategically beyond technical IT tasks.

---

15 In the US, the National Security Agency and the Department of Homeland Security accredit university and college courses. To date, they have accredited over 200 courses. In the UK, the National Cyber Security Centre, a government body, certifies cyber security degrees. To date, it has accredited over 25 postgraduate degrees.

16 Cyber Security Challenge UK (2017), 'Barclays delivers skills boost with Cyber Challenge UK competition', available at: **https://www.cybersecuritychallenge.org.uk/news-events/barclays-delivers-skills-boost-cyber-security-challenge-uk-competition**.

17 Office of the Chief Scientist (2015), *STEM-trained and job-ready.* Available at: **https://www.chiefscientist.gov.au/sites/default/files/OPS12-WIL_web.pdf**.

Various models of industry placement could easily be adapted to cyber security education in Australia. For example, industry-funded scholarship programs, known to some universities as 'co-op' scholarships, have been used effectively in disciplines such as information systems, accounting and engineering. The UK has improved the availability of work-integrated learning by developing professional apprenticeships, including in cyber security, where students combine employment with part-time study to achieve a diploma or bachelor-level qualification. Australia is currently piloting higher apprenticeships with one stream of IT apprenticeships.[18] The pilot program has been running since 2016, and 200 apprentices will complete the program at the end of 2018. AustCyber has commenced discussions about setting up a cyber security apprenticeship stream in this program.

It is critical to enable more workers to transition into cyber security

Given the time lag for the formal education system to graduate students from specialist cyber security qualifications, workers with applicable skills-sets who may want to transition into a cyber security work role will be very important to grow the cyber security workforce in the near-term. While graduate supply is now accelerating and provides a clear path to close the gap between demand and supply in cyber security skills, it will take some time until the supply pipeline of graduates is large enough to fully meet workforce demand (see Figure 35). To close the cyber security skills gap in the short- and medium-term, workers from the broader IT sector and other industries with relevant knowledge, skills and abilities will need to transition into the cyber security workforce.

Figure 27

Cyber workforce demand and supply

Number of workers, 2017–2026
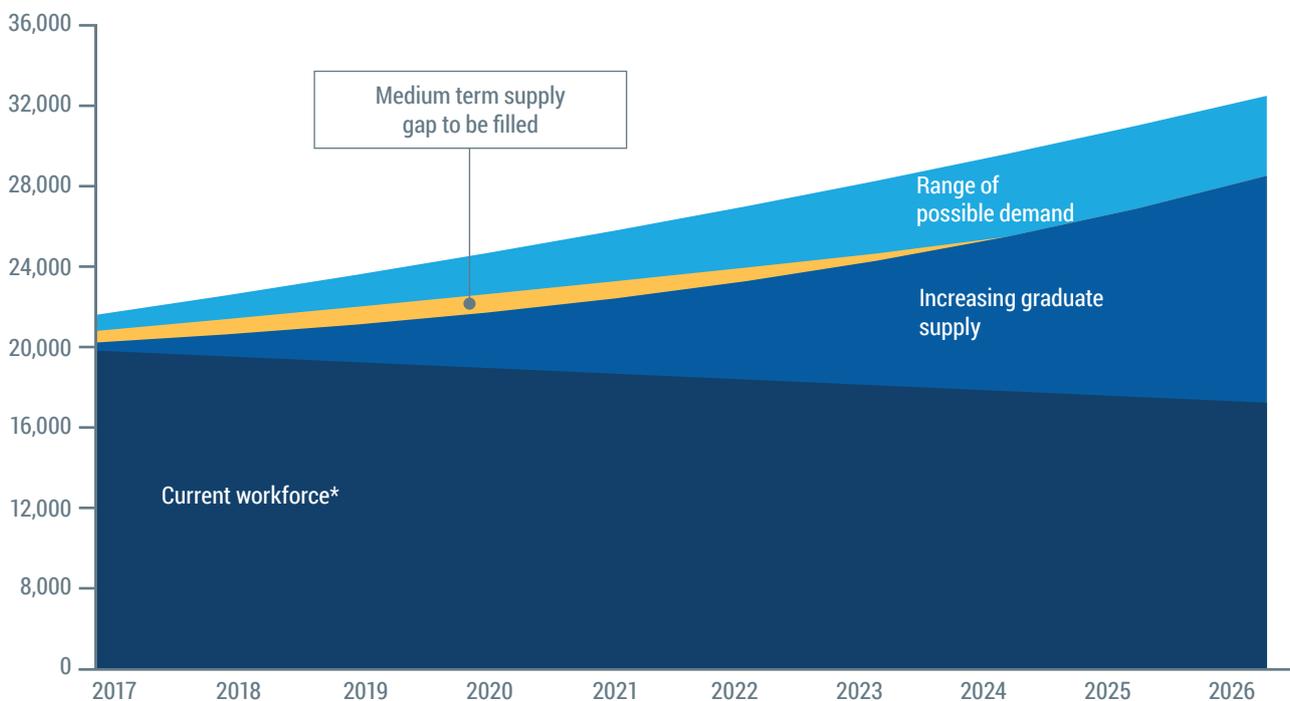
* Current workforce is shrinking due to natural retirements and net loss of workers overseas
SOURCE: AlphaBeta analysis, Gartner, interviews

18   Further information on the Apprenticeship Training – alternative delivery pilots is available at: **https://www.australianapprenticeships.gov.au/programs**.

3 THE CHALLENGE: AUSTRALIA NEEDS TO PLUG THE WORKFORCE GAP, REMOVE STARTUP BARRIERS, STRENGTHEN R&D, AND MEASURE GROWTH AND IMPACT

As detailed in Figure 28, a breakdown of the IT occupations most relevant to the technical roles required in the cyber security workforce reveals a large stock of IT workers with potentially transferable skills. People in IT occupations who are highly suited for a career shift to cyber security include Software and Applications Programmers, IT Support Technicians, and IT Managers. Workers from other industries with experience in risk oversight, regulatory management and incident response could also potentially transition into cyber security. This may include lawyers, people in risk management, and communications professionals.

There is a significant opportunity to adapt the skills of existing IT professionals to enable them to take up more specific cyber security roles

Between 2011 and 2016, more than 70 per cent of workers who became IT Security Specialists (the only cyber security-specific occupation classification currently tracked by the Australian Bureau of Statistics) came from other IT occupations. This is a strong sign that there is a large pool of workers currently employed in the broader IT sector with transferrable skills and who could transition into more specific cyber security roles. Most of those who transitioned between 2011 and 2016 were IT and Telecommunications Technicians, followed by IT Network and Support Professionals, and Systems Analysts Programmers.

However, it is also evident that there is a lack of workers transitioning into the cyber security sector from industries outside IT. This is largely because current recruiting practices still place strong emphasis on technical skills. This is despite the well-acknowledged need to improve the 'soft skills' and diversity of workers in the sector. There is also a lack of public understanding of the range of different career paths spanning technical and non-technical cyber security roles.

Figure 28

Employment in the top 5 occupations relevant to cyber security
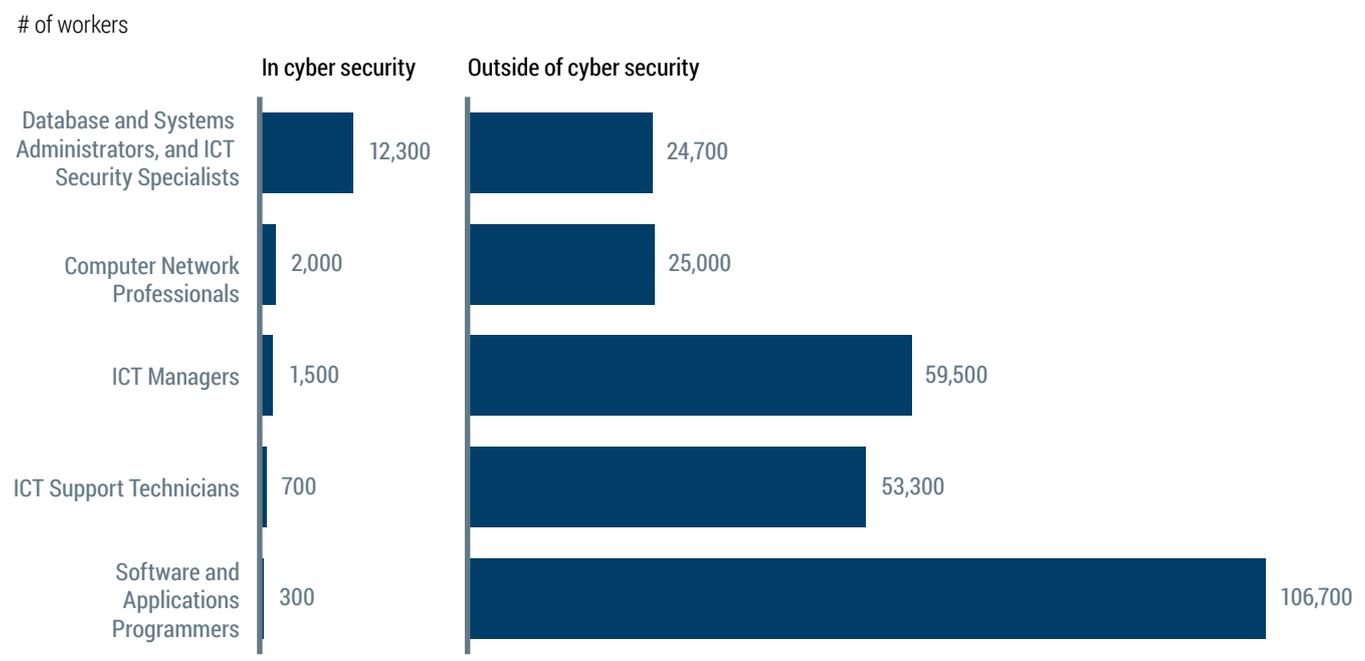
# of workers

SOURCE: Gartner; Australian Bureau of Statistics; TalentNeuron; AlphaBeta Analysis

The new national vocational training curriculum in cyber security is opening up new pathways for workers from other industries to transition into the cyber security sector. Early evidence suggests that students opting for the new vocational cyber security training are older than the average vocational education and training student. At two of the institutions offering the courses, more than half this student cohort was over 30.

'The average age is 30 to 35 in our courses. Students are coming from diverse backgrounds wanting to develop skills in cyber security.'
Vocational education and training manager

Ensuring training options for transitioning workers, while critical, is not sufficient. A number of other enablers need to be in place to support workers to transition into the cyber security sector.

Employer-led transition is currently limited to larger organisations

Interview evidence suggests that at the moment the greatest emphasis on transition into cyber security is employer-led, or within organisations. This is a critical mechanism to facilitate transition, as employers are well-placed to guide and fund workers through the transition journey. Large employers (for example, banks and government) in particular have the greatest capacity to transition their workforces as they have the scale and resources necessary to offer internal mobility to their workers. Transition within small to medium-sized organisations is more limited but could be boosted if these companies have access to clear transition models that help them identify target workers, assess what additional skill-sets they require, and find the means internally or externally to skill them appropriately.

Large organisations that are already successfully training workers from various backgrounds to shift into cyber security roles have identified five steps for effective workplace transitions:

1. Map out the cyber workforce needs of the organisation over the next two to three years, using a skills framework if helpful, and identify roles that can be effectively filled with transitioning workers.

2. Identify sources of high potential, non-cyber employees who could transition to cyber. Key functions to look for within the organisation are IT, risk management, communications and legal.

3. Offer an attractive opportunity to potential cyber employees including a clear career path, training opportunities, good salary and engaging job tasks/activities. The fast growth of cyber may also offer faster progression to management opportunities than other functions within the organisation.

4. Train and support transitioning workers through internal mentoring and on-the-job training, and private internal or external short-course training programs, such as SANS or micro-credentials. Many organisations are using executive education courses instead of full university degree courses to train workers in transition. This is because university degrees tend to take longer and cost more than executive education.

5. Leverage the newly transitioned workers to provide mentoring to the next 'tranche' of potential cyber employees, allowing rapid scaling of the workforce.

Further developing these steps into a model for employer-led transition that small to medium-sized organisations can quickly apply, and socialising through industry associations will support improved flow of workers through employer-led transition programs.

Worker-led transition requires better access to information and training, and more support from employers

Worker-led transition is also a key mechanism to help bridge the cyber security skills gap. It has substantial potential to scale (as it draws upon a wide pool of potential workers across the economy) but it is more complex that employer-led transition. Workers must independently move through several stages, as illustrated in Figure 29. They must independently gather information on transition, undertake training, and find employment in the cyber security workforce, bearing the full burden and costs of transition themselves.

A worker's progress through the transition journey relies on several enablers at each stage. For example, at the beginning when a worker considers transitioning they require information on the cyber security sector – what it is, why it matters, the wages offered and potential career paths. Further down the transition journey, they need an understanding of their skills match, training requirements, access to training places and job placement services.

Figure 29

The transition journey – worker-led transition

Supply of high potential workers	Worker considers transitioning to cyber security	Worker gathers information on transition	Worker undertakes training program	Worker finds employment in cyber
• Workers with high skills match with cyber security roles • Workers in equivalent occupations in different industries, e.g. ICT	**Enablers**			
	• Ability to absorb income loss during retraining • Attractiveness of cyber careers • Positive attitudes about cyber work • Access to information about cyber roles and career	• Understanding of training requirements • Understanding of their existing skills match and any gaps • Access to information on available training programs	• Availability of training places that ensure job-readiness • Affordability of training places	• Readiness of employers to support transitioning workers with additional on-the-job training • Attitude of employers • Employer recognition of training, particularly training independently pursued by workers

SOURCE: Expert interviews

The most critical enabler to facilitate transition is access to information (such as cyber careers and pathways), training access, training affordability, and employer attitudes.

Information access: Currently there is very limited information available to those outside the cyber sector on cyber careers and the sector more broadly. The available information is scattered, not necessarily cyber-specific, and not tailored for people unfamiliar with the sector. There is an opportunity to build on existing platforms for example, the Government's JobOutlook website hosts information on IT occupations – including ICT Security Specialist.[19] This includes information about average weekly pay, future growth, and degree levels required. Enhancing this to include information on career pathways and broader work roles that require cyber security skills would assist people considering a transition to the sector.

In addition, there is no clear source of information to help potential workers understand the training requirements for different cyber roles. This increases uncertainty around the transition process and amplifies risk that workers who could transition into a cyber security role will not have the required information to make an informed decision.

Workers considering a career change into cyber security need a centralised source of information about pathways into the sector. Cyberseek, funded by NICE in the US, is a good example.[20] It provides up-to-date data on supply and demand in the US cybersecurity job market via interactive visual tools, including heat maps that show worker demand and supply per state. The website also outlines cyber security career pathways and offers key information such as average salaries, required skills/certifications, and the number of job openings. Australia could explore implementing a similar tool to Cyberseek.

19   For more information see: www.joboutlook.gov.au.
20   For more information see: www.cyberseek.org.

Figure 30

Costs of different cyber training programs

Total costs of different cyber training programs	Course length	Share of cyber training places
$, 2017–18	Months	%

Program	Cost	Course length	Share
Master's Degree/Grad Diploma	40,000 – 55,000	18–24	~20
Bachelor's Degree (generally not for transition workers)	27,000 – 30,000	36	~35
Advanced Diploma	10,000 – 18,000	12	~10
Graduate Certificate	7,200 – 13,000	6–12	~15
VET Cert IV	1,800 – 8,000	6–12	~15
VET Short Course	600 – 700	< 3	~5

Note: The low cost estimate for the Adv. Diploma and Cert IV is Government subsidised, while the high estimate is full fee paying. The Bachelor's degree fee is for a Commonwealth Supported Place.
SOURCE: University and TAFE websites

Affordability of training: Training affordability is also a key issue for worker-led transition. While course numbers and places have grown rapidly in recent years, the majority of cyber training places are still concentrated in longer, more expensive courses, such as bachelor's or master's degrees, which can cost $30,000 to $55,000 (see Figure 30).

Even though these course fees can usually be deferred through FEE-HELP, accumulating transition-related debts could be a barrier to workers shifting to cyber. More intensive, shorter courses of good quality would ease the transition burden for potential workers and help stimulate the supply of cyber workers in the short- to medium-term. This would also minimise the costs to employers from employer-led transition, as training costs would be lower, workers would not need to take as much time away from work to retrain, and they would transition faster.

Universities and TAFEs are not the only institutions with a role to play. There is scope for select high-quality private providers of niche cyber security education and training to supplement the selection of short courses currently on offer. Private sector training organisations such as Ionize and UXC Saltbush provide training for the Australian Signals Directorate's Information Security Registered Assessors Program (IRAP). Overall, however, there is still plenty of scope for high-quality training providers as well as universities to broaden their course offering to include shorter, more targeted cyber security training to help with the transition process.

3 THE CHALLENGE: AUSTRALIA NEEDS TO PLUG THE WORKFORCE GAP, REMOVE STARTUP BARRIERS, STRENGTHEN R&D, AND MEASURE GROWTH AND IMPACT

Employer attitudes: Industry interviews suggest that employers, especially small to medium-sized organisations, are still reluctant to hire transitioning workers. Employers perceive these potential workers as risky prospects, lacking experience and job-readiness. To help resolve the cyber skills gap, employers need to broaden their hiring strategies. Instead of relying on rigid 'check-box' recruiting that focuses heavily on work experience, employers need to look for translatable skills for specific cyber security work roles as a way of identifying promising candidates.

To help resolve the cyber skills gap, employers need to broaden their hiring strategies.

A transition model for employers could help in this respect. A clear transition blueprint for companies of different sizes would minimise the risks associated with identifying suitable workers and training them appropriately.

Placement services could also have a role in changing attitudes within the sector. Given their intimate knowledge of recruiting and their relationships with companies, they could be influential in challenging the prevailing recruitment methods, which over-emphasise technical skills and experience. Some placement services are already using unorthodox approaches to change employer perceptions, pitting their transitioning cyber candidates against in-house cyber teams of major companies in hackathons to demonstrate their capabilities.

The section *Make Australia the leading centre for cyber security education* in Chapter 4 lists a range of actions that could help Australia build a strong, high-quality cyber education system, including support for educational infrastructure and expansion of school programs to build a talent pipeline.

Box 11

Schools Cyber Security Challenges: Building the cyber workforce of the future, today

There is a significant lack of awareness and skills around cyber security in society, the workforce and amongst our nation's students.

Constantly evolving cyber attacks continue at pace, directed at all kinds of organisations, including government departments, businesses. Schools are also susceptible to malware threats as students and staff bring connected devices from home and share information across their networks.

Educating young Australians about the risks they face online is important, but so is offering them the opportunity to learn about cyber security at a deeper level, enabling them to have cyber skills for life.

The Schools Cyber Security Challenges is Australia's first cross-industry collaboration of its kind.

The program aims to close the growing gap in cyber security awareness and skills amongst Australian students by ensuring it becomes an education-critical subject area.

Developed by the Australian Computing Academy at the University of Sydney, in partnership with AustCyber, ANZ Bank, BT, Commonwealth Bank, National Australia Bank and Westpac, the program equips Australian high school teachers to teach vital cyber security skills to years 7–10 students, via engaging and relatable classroom challenges.

'Increasingly, every aspect of our lives is digitally enabled or interconnected in some way,' says Richard Johnson, CISO at Westpac. 'The opportunity to build cyber security skills and awareness in children coming through school – young people who are already digitally savvy – then have them enter the workforce is a great step forward.'

The challenges are an innovative ground up approach designed to provide high school teachers with resources to support the teaching of cyber security concepts, and to inform students of career opportunities in the field.

Delivered free of charge, the challenges explore general topics including personal information security and data sharing, as well as technical topics such as cryptography and network security. The range of engaging activities involve investigation, deduction and programming to develop student knowledge, skills and dispositions as they work their way through increasingly difficult problems.

The challenges are classroom ready and aligned with both the Australian Curriculum: Digital Technologies and the ICT Capability for schools.

The official launch event was hosted in Sydney in February 2019 and garnered extensive media coverage and attention. Cyber security roadshows have been held in major cities across Australia.

Over 45,000 students and 2,500 teachers have participated in at least one of the four challenges, with approximately half of them completing multiple activities.

By creating security-conscious students who are well equipped and able to adopt lessons learned to their personal lives the workforce, this will help to build a critical pipeline of cyber security skills in Australia.

Schools
Cyber Security
Challenges

3.3   RESEARCH AND COMMERCIALISATION

Cyber security companies are operating in a competitive and rapidly changing market environment, in which technology is a key ingredient for success. The growing sophistication of cyber adversaries forces security providers to constantly stay ahead of the curve by developing ever-more innovative products. Australia's cyber security research capability is strong. However, several factors undermine the country's innovative strength. Australia lacks nationally coordinated and collaborative R&D in cyber security. Another major problem is the difficulty for many researchers to turn new and innovative technologies into marketable products that truly meet customer needs. To improve this technological transition, Australia needs to strengthen its pre- and post-R&D activities, such as supporting researchers to engage with industry to identify problems and reach out to potential investors.

Australia lacks nationally coordinated and collaborative R&D in cyber security

Competitiveness in cyber security is highly dependent on R&D

Australian cyber security providers can compete on price or on value – for example, by providing products that are easier to use or technically more advanced, or by offering stronger support services.

Australian providers can also compete on scope, for example, by offering a more comprehensive array of products and services. Analysis of the attributes that matter most to cyber security customers when choosing a vendor gives valuable insight into what makes a cyber security company competitive.

A survey of leading CIOs and CISOs for this Sector Competitiveness Plan reveals that customer appeal of cyber security companies largely hinges on technological leadership (see Figure 31). This is particularly true for software. Australian CIOs and CISOs overwhelmingly said they consider effective technology the most important factor when weighing the purchase of cyber security software.[21]

---

21   AlphaBeta/McKinsey (2017), 'Survey of Australian CIO and CISO purchasing factors'.

Box 12

Laava: Unique smart fingerprints on every 'thing', developed through world-leading cyber security R&D

Laava has developed Smart Fingerprints® and the Authentication of Things® Platform to enable the trusted authentication of any document or product at scale and at low cost. Laava's objective is to help Australia create a high trust ecosystem and boost Australia's reputation as a high-integrity source of services and goods.

More than ever, consumers want products that have transparent origins, provenance and contents. Consumer concerns about sustainability increasingly shape the market. Food suppliers and retailers need to respond to increasing demands from consumers for more information to help them make responsible choices about the products and services they buy.

Laava's technology will help combat counterfeiting, currently representing an estimated 3.3 per cent of world trade and projected to drain US$4.2 trillion from the global economy by 2022. Online counterfeiting losses alone were US$323 billion in 2017. But it is more than money – fake medicines are responsible for over one million deaths annually.

Only 33 per cent of consumers in the United States are confident in the safety of their food, 67 per cent of consumers want to know what goes into their food, and 50 per cent say it influences decisions. Traceability, provenance and proof of claim are now becoming entry requirements for premium products. Eight out of 10 consumers trust a brand more if it offers more transparency about its contents and provenance than competitors, and 9 out of 10 consumers want access to this information on their phones.

Laava Smart Fingerprints® are a brandable, visual 'mark of trust'. They drive the Laava Authentication of Things® platform which provides end-to-end security. Laava's Smart Fingerprints® provide a second generation alternative to first generation Quick Response (QR) codes but are more secure, flexible and visually distinctive with product branding.

QR codes are visually indistinct from each other so the naked eye can't easily tell them apart and are ill-suited for authentication. They contain hidden instructions which are machine-readable codes people cannot read and are highly vulnerable to exploitation and abuse.

QR technologies embed codes leave the scanning user completely unprotected. Just one scan can instantly direct your phone to unsafe places, containing viruses or scams, and lead to identity theft and other bad outcomes. QR are easy to copy and spoof, and anyone generate them with a free app – including countless malicious actors.

Laava's Smart Fingerprint® contains no hidden code – protecting users. Every Smart Fingerprint® is cryptographically generated as a once-only visual image, which a camera equipped phone can capture optically using computer-vision technology. Smart Fingerprints® are scannable through a simple web scanner, a standalone app or WeChat app.

Every single individual Smart Fingerprint® is created once and never repeated.

Once scanned, Laava then matches that image on its secure servers to authenticate it before it allows any content to be transmitted.

For the cost of a printed label, Laava bridges the gap between a physical thing and the story behind that thing, it's provenance and its digital credentials.

Laava partnered with AustCyber to develop this technology. 'Not only did AustCyber assist with the funding of our technology development and research in key areas, AustCyber also helped us to identify and communicate our value propositions to multiple parties in industry and government agencies, such as Austrade,' says Laava Co founder Tony Surtees. 'This has been essential to the commercialisation of our key research insights and transforming us into a viable early-stage growth business with real-world product and users.'

Figure 31

Most relevant purchasing factors for organisations when selecting a cyber security products vendor, 2017*

Relevance in purchasing decisions (0–10, 10=most relevant)
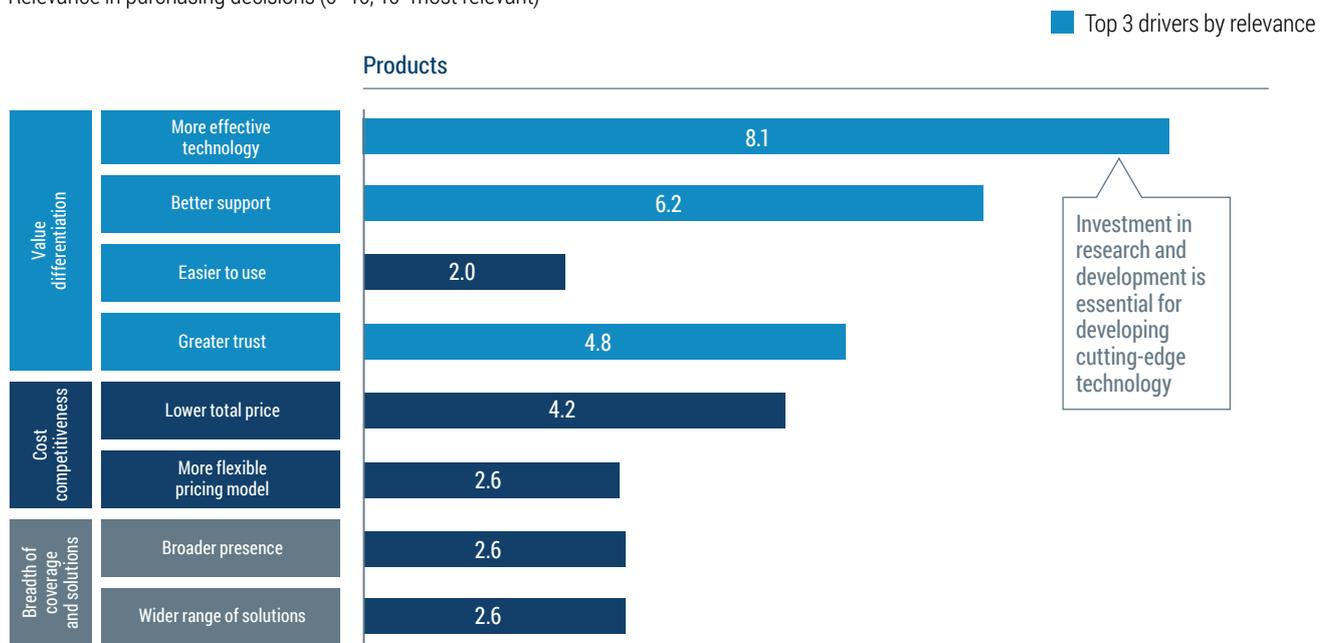
■ Top 3 drivers by relevance

Products

Value differentiation	More effective technology	8.1
	Better support	6.2
	Easier to use	2.0
	Greater trust	4.8
Cost competitiveness	Lower total price	4.2
	More flexible pricing model	2.6
Breadth of coverage and solutions	Broader presence	2.6
	Wider range of solutions	2.6

> Investment in research and development is essential for developing cutting-edge technology

* CIOs and CISOs were asked to allocate 100 points across the drivers that are most relevant for them when assessing cyber security vendors

SOURCE: AlphaBeta/McKinsey (2017), Survey of Australian CIO and CISO purchasing factors

'Tech is essential, but it has to be effective and tailored to our problem. Many companies focus on technological edge without solving a real problem for their customers.'
Australian private sector CISO

Unearthing new ideas

Developing effective technologies is resource-intensive because it requires companies and research institutions to invest heavily in R&D and collaborate to unearth new ideas and commercialise them. Governments can support these efforts, either directly through research grants and targeted funding programs or indirectly via R&D tax incentives. For example, governments can provide funds to research institutions or government agencies with the aim of boosting R&D. Governments can also fund programs to improve research collaboration between universities and industry.

Translating ideas into products

Post-R&D activities are equally important. The most innovative idea will fail to make an impact if it finds no user. Researchers and inventors need strong support from government funding agencies and industry partners to improve the success rate of transitioning innovative cyber security technologies into real world products that customers want to buy.[22] This will involve broadening the scope of transition activities and exposing new technologies and tools to a wider audience. Australia could do more to bridge the gap between researchers and vendors, sometimes described as a 'valley of death'.

Leading countries in the global market for cyber security software, such as the US and Israel, are conscious of the link between technological innovation and market success, and invest heavily in R&D.

---

22 Maughan, D., et al. (2013), 'Crossing the "Valley of Death": Transitioning Cybersecurity Research into Practice', *IEEE Security & Privacy*, Vol. 11, No. 2, pp. 14–23, March–April 2013. Available at: **http://www.csl.sri.com/papers/ieee-sp-tt-2013/ieee-sp-tt-2013.pdf**.

Figure 32

Global cyber security software market share by company domicile

% 2015

Rest of world 18%

United Kingdom 3%

Israel 18%

US$26.4B

United States 61%
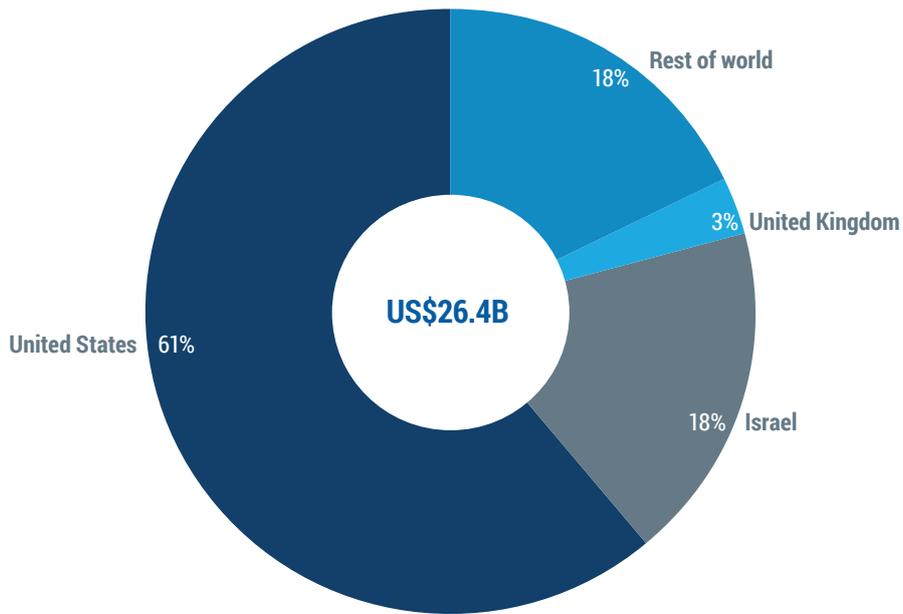
SOURCE: IDC Worldwide Security Software tracker; AlphaBeta and McKinsey analysis

For example, the market power of American cyber security software companies coincides with a significant commitment to R&D. These companies are the leading vendors in the global market, generating 61 per cent of the US$26.4 billion of total cyber security software sales worldwide in 2015, as shown in Figure 32. They invest more than US$200 million each year to invent and develop new cyber security technologies. The US government adds further weight to the sector by providing additional R&D funding of more than US$500 million per year.

Israel, traditionally boasting some of the highest defence spending in the world, also provides strong government support for cyber security R&D. Israeli companies form the second-strongest vendor group in the global market for cyber security software, accounting for 18 per cent of total sales worldwide. Israel's Office of the Chief Scientist is frequently cited as the country's largest single investor in cyber security research, but official budget numbers are not readily available.

3 THE CHALLENGE: AUSTRALIA NEEDS TO PLUG THE WORKFORCE GAP, REMOVE STARTUP BARRIERS, STRENGTHEN R&D, AND MEASURE GROWTH AND IMPACT

Several other countries have begun to catch up in recent years, but their R&D budgets for cyber security still appear modest compared to US and Israel. For example:

- The United Kingdom government has developed a Defence and Cyber Innovation Fund worth more than US$200 million (GB£165 million) to develop innovative cyber security technologies and products. The investment is part of the country's National Security Strategy, which will inject the equivalent of US$2.37 billion (GB£1.9 billion) into the British cyber security sector through to 2021. Some of the money will fund 'cyber startups and academics to help them commercialise cutting-edge research and attract investment from the private sector'.[23]

- The Government of Singapore recently announced a five-year plan to build new R&D expertise and improve its cyber security capabilities. The National Cybersecurity R&D Programme is investing around US$20 million per year (equivalent to S$130 million over the five years) in cyber security research and innovation.[24]

> Several potential sources of finance for cyber security research remain largely untapped

- The Australian Government has made cyber security a national priority for science and research. Current expenditure on cyber security R&D, as shown in Figure 33, is estimated to be approximately A$81 million per year, which excludes R&D support through the national R&D tax incentive and research block grants to universities.[25]

Cyber security research needs a stronger focus

Australian organisations undertaking cyber security R&D need to be more competitive for public research funding, for example, by better articulating commercialisation pathways and the potential for economy wide benefits. Similarly, funding agencies could improve their understanding of cyber security's importance to the entire Australian economy, and how improving our cyber security R&D outcomes would make Australia a world leader. A breakdown of available grant schemes, as shown in Figure 33 indicates several potential sources of finance for cyber security research remain largely untapped.

Block grants to universities are generally the most important channel to directly fund R&D activities in Australia. In 2015, the Australian Government granted universities almost A$1.8 billion to support their R&D work. Block grants are awarded on a yearly basis based on a university's performance in attracting research income and the successful completion of higher degree by research students. When awarded block grant funding, universities have complete autonomy in deciding how the grant is administered across its research portfolio.

However, due to difficulties in collecting block grant data, the extent to which these funding tools are currently used to finance cyber security R&D is unclear. It is fair to assume, however, that Australia still has scope to increase the use of university block grants for cyber security R&D funding A new industry-led Cyber Security CRC, announced in late 2017, will be critical to strengthening Australia's cyber security R&D capabilities. The Australian Government will invest $50 million in the Centre over the seven years to 2024. This is in addition to about $90 million in funding from a consortium of 25 government, research and business partners led by the Cyber Security CRC. The CRC represents a coordinated research effort focused on delivering real-world cyber security solutions (Box 13).

23 British Government (2016), National Cyber Security Strategy 2016–2021. Available at: https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy.
24 Singapore Government (2017), *National Cybersecurity R&D Programme.* Available at: https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme.
25 Australian Government (2016), *Cyber Security – Capability Statement.* Available at: http://science.gov.au/scienceGov/ScienceAndResearchPriorities/Pages/Cybersecurity.aspx.

Existing and potential sources of funding for cyber security R&D in Australia#

2016–17, A$ millions   ■ Existing funding   ■ Potential sources of funding

A$99m in funding has been granted since 2015 in Accelerating Commercialisation Grants, none of which has been awarded to cyber security companies

81	35	150	160	200	744	1,778
Federal Government-funded R&D†	Entrepreneurs' Programme	Cooperative Research Centres	Defence Industry and Innovation Programmes	CSIRO Innovation Fund§	ARC grants	Research block grants

*   Does not include the R&D Tax Incentive

†   Total funding for cyber security research as reported by the Federal Government, excluding research block grants and the R&D Tax Incentive; may be some overlap with ARC grants

§   Total capitalisation of the Fund, not annualised funding

SOURCE: Innovation and Science Australia; Australian Gov Science and Research Priorities 2015 Report; press search; AlphaBeta and McKinsey analysis

The Department of Defence is another major potential funding source for cyber security research. In the fiscal year ending June 2017, the Department paid businesses, academia and research organisations an estimated A$160 million to help develop new, innovative technologies for military use.[26] The Department's Defence, Science and Technology Group, the second largest publicly funded R&D organisation in Australia, just launched the Next Generation Technology Fund, which can invest over $730 million over the decade to June 2026 into emerging early-stage technologies of strategic value to Australia's defence forces. Cyber security is one of the fund's nine priority areas.

Cyber security researchers may also be able to make better use of the CSIRO Innovation Fund. This joint government-private sector initiative invests in startup, spin-off companies and existing small- to mid-sized enterprises, to improve the translation of publicly funded research into commercial outcomes and stimulate innovation in Australia.

Accelerating commercialisation is an area of focus across Australian Government with the aim of helping small and medium-sized businesses to commercialise novel products, processes and services. Around 180 companies received financial assistance between 2015 and early 2017 through a competitive grants process, with a total value of A$99 million.[27] Cyber security companies did not received any assistance from this program over that period, which may be due to a lack of quality applications.

Grants provided by the Australian Research Council (ARC) form the second largest source of direct R&D funding in Australia. Yet analysis of the ARC's funding pattern over the past decade reveals that only a fraction – around 0.6 per cent of the ARC's annual grant budget (A$744 million in 2016) – was used to fund research projects related to cyber security.[28] Postgraduate training centres and research hubs can apply for ARC funding through the Industrial Transformation Research Program (ITRP), which now lists cyber security as an Industrial Transformation Priority.

26   Innovation and Science Australia (2016), *Performance Review of the Australian Innovation, Science and Research System*. Available at: https://www.industry.gov.au/sites/default/files/2018-10/performance-review-of-the-australian-innovation-science-and-research-system-isa.pdf.

27   Australian Government Business (2017), 'Accelerating Commercialisation funding offers'. Available at: https://www.business.gov.au/Assistance/Accelerating-Commercialisation/Accelerating-Commercialisation-funding-offers.

28   ARC (2016), 'Grants Dataset'. Available: http://www.arc.gov.au/grants-dataset.

Australian Government
invested
$50 million
over seven years

Almost
$90 million
contributed from
a consortium of
25 industry, research and
government partners
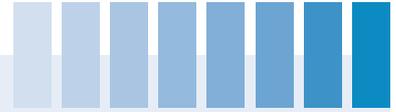
Box 13

Australia's Cyber Security CRC

Australia's Cooperative Research Centre (CRC) Program has become a proven model for funding joint research and development between government, businesses and researchers. Participants include private sector organisations (both large and small enterprises), industry associations, universities and government research agencies such as the Commonwealth Scientific and Industrial Research Organisation (CSIRO).

It aims to develop and commercialise solutions for industry-specific problems, and ultimately improve the competitiveness, productivity and sustainability of Australian industries. CRCs are particularly relevant in sectors where Australia already has a competitive strength. For example, current CRCs cover areas such as advanced manufacturing, plant biosecurity and medical technologies.

Acknowledging that cyber security is a strategic priority, the Cyber Security Cooperative Research Centre (CSCRC) was established in 2018 to develop innovative projects that strengthen the nation's cyber security capabilities. The CSCRC is a non-profit public company and combines $50 million in funding from Australian Government with additional industry and university participant funding over seven years to 2025.

The CSCRC works with 24 participant organisations including:

- seven government departments or agencies;
- CSIRO's Data61;
- six research providers; and
- ten businesses (from large organisations to small-to-medium cyber security businesses).

On launching the CSCRC, the Australian Government said the CRC will contribute to the country's reputation as a secure and trusted place to do business. It will also deliver broad economic benefits by enabling industry to attract and increase investment, trade and commerce.

'Research at the CSCRC focuses on delivering real-world cyber security solutions,' says the CEO of the Cyber Security CRC, Rachael Falk. 'The Cyber Security CRC is very industry driven – we're focused on delivering research with impact and solving real-world cyber security problems. We want to deliver innovative solutions to industry, government and all Australians. We also want to inspire the next generation of cyber security professionals by offering scholarships through our participating universities and the opportunity to learn from some of the best cyber security researchers in Australia.'

Figure 34

Quality measures of Australia's research performance

Dimension		Description	Ranges of performance
Overall rating	Activity	Share of total world publications (%)	37th ————————————————●9th———————— 1st
	Consistency in quality	Quality across different research dimensions	120th —————————————————————————●1st— 1st
	Relevance	Relative citation impact (# of citations/# of publications)	37th —————————————●14th———————————— 1st
	Distinctiveness	Share of world's 1% highest cited publications	37th ——————————————————●7th————————— 1st
Cyber security-specifc rating	Patent fillings	Patent fillings in Cyber Security research	120th ——————————————————————●4th——— 1st
	Relevance	Relative citation impact (# of citations/# of publications)	120th ——————————————————————————●1st 1st

SOURCE: Australian Government Science and Research Priorities 2015; Thompson Reuters InCites; Austrade; LexInova; AlphaBeta and McKinsey analysis

Blockages to cyber security innovation in Australia

Australia is home to 43 universities. They carry out most of the foundational research and have access to a significant amount of funding relative to other OECD nations.[29] Cyber security research from Australia ranks highly in global comparison, Figure 34 reveals.

In terms of citation impact – an indicator of research quality – cyber security research papers from Australia are the most heavily referenced in the world, according to Thomson Reuters data.[30] Australian universities appear well placed to lead the knowledge creation and spearhead the invention of new technologies in cyber security.

Cyber security research papers from Australia are the most heavily referenced in the world

Many universities in Australia are already regarded as global research leaders in fields with cyber security applications, such as packet switching (a technology that breaks down data into smaller parcels before transmitting them), quantum cryptography, distributed computing and wireless security technology. The Australian National University and the University of New South Wales are already at the leading edge of global research into quantum computing and its potential applications for the cyber security sector.

---

29   Innovation and Science Australia (2016).
30   Referenced in Australian Government (2016), *Cyber Security – Capability Statement*.
     Available at: **http://science.gov.au/scienceGov/ScienceAndResearchPriorities/Pages/Cybersecurity.aspx**.

Box 14

Australia's lead in the global quantum race

It is the nightmare of anyone guarding top secret data: a machine so powerful that it could crack even the toughest security codes. Quantum computers could do just that. They exploit the strange behaviour of tiny atoms, better known as quantum physics, to solve problems immensely faster than the world's fastest supercomputers. This makes them a huge threat for current encryption methods – in theory, at least, because no one has yet managed to build such a code-breaking quantum computer.

The existence of quantum computers was long thought to be a distant vision. However, rapid technological advances by IBM, Google and others have raised concerns that quantum computers may become a reality much sooner. The National Security Agency in the US recently warned that the time to act and build 'quantum-resistant cryptography' is now[31] The Canada-based Global Risk Institute puts the odds of a quantum computer cracking key security algorithms by 2031 at 50 per cent.[32]

Many countries, including Australia, Canada, the US, Singapore and Japan, have increased their technology investments in recent years, fuelling a global race to develop the world's first viable quantum computer. At the forefront is a network of 180 researchers from six Australian universities (University of New South Wales, Australian National University, University of Melbourne, University of Queensland, Griffith University and University of Sydney), the Australian Defence Force Academy, and a dozen international university and industry partners.[33]

The network is coordinated through the Australian Research Council Centre of Excellence for Quantum Computation and Communication Technology, or CQC2T.
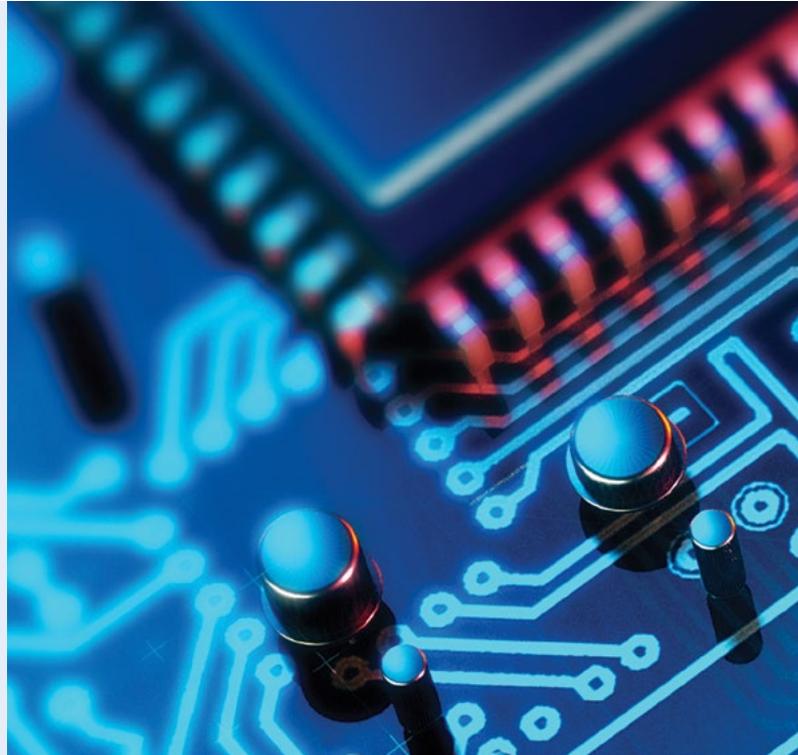
While scientists around the globe are exploring a range of exotic materials – from synthetic crystals to dye pigments – to build a quantum computer, Australia's CQC2T research group is on track to develop the world's first quantum computer in silicon.

'Our Australian centre's unique approach using silicon has given us a two to three-year lead over the rest of the world,' says Professor Michelle Simmons, director of CQC2Tsays Professor Michelle Simmons, director of CQC^{2}T.[34] 'These facilities will enable us to stay ahead of the competition.'

Funded with more than A$100 million worth of government grants and investments from Telstra and the Commonwealth Bank of Australia, CQC2T's work is crucial for Australia's nascent cyber security sector.[35]

31 National Security Agency (2016), *Information Assurance Directorate. Commercial National Security Algorithm Suite and Quantum Computing FAQ*. Available at: https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf.
32 Global Risk Institute (2016), 'A quantum of prevention for our cyber-security'. Available at: http://globalriskinstitute.org/publications/quantum-computing-cybersecurity/.
33 UNSW (2016), 'Backgrounder: Quantum computing at UNSW and timeline of major scientific and engineering advances'. Available at: https://www.science.unsw.edu.au/news/backgrounder-quantum-computing-unsw-and-timeline-major-scientific-and-engineering-advances).
34 UNSW (2016), 'Prime Minister hails UNSW's quantum computing research as the world's best'. Available at: http://newsroom.unsw.edu.au/news/science-tech/prime-minister-hails-unsws-quantum-computing-research-worlds-best.
35 Greg Hunt, then Australian Minister for Industry, Innovation and Science (2016), 'Major leap forward for Australian quantum computing'. Available at: http://minister.industry.gov.au/ministers/hunt/media-releases/major-leap-forward-australian-quantum-computing).
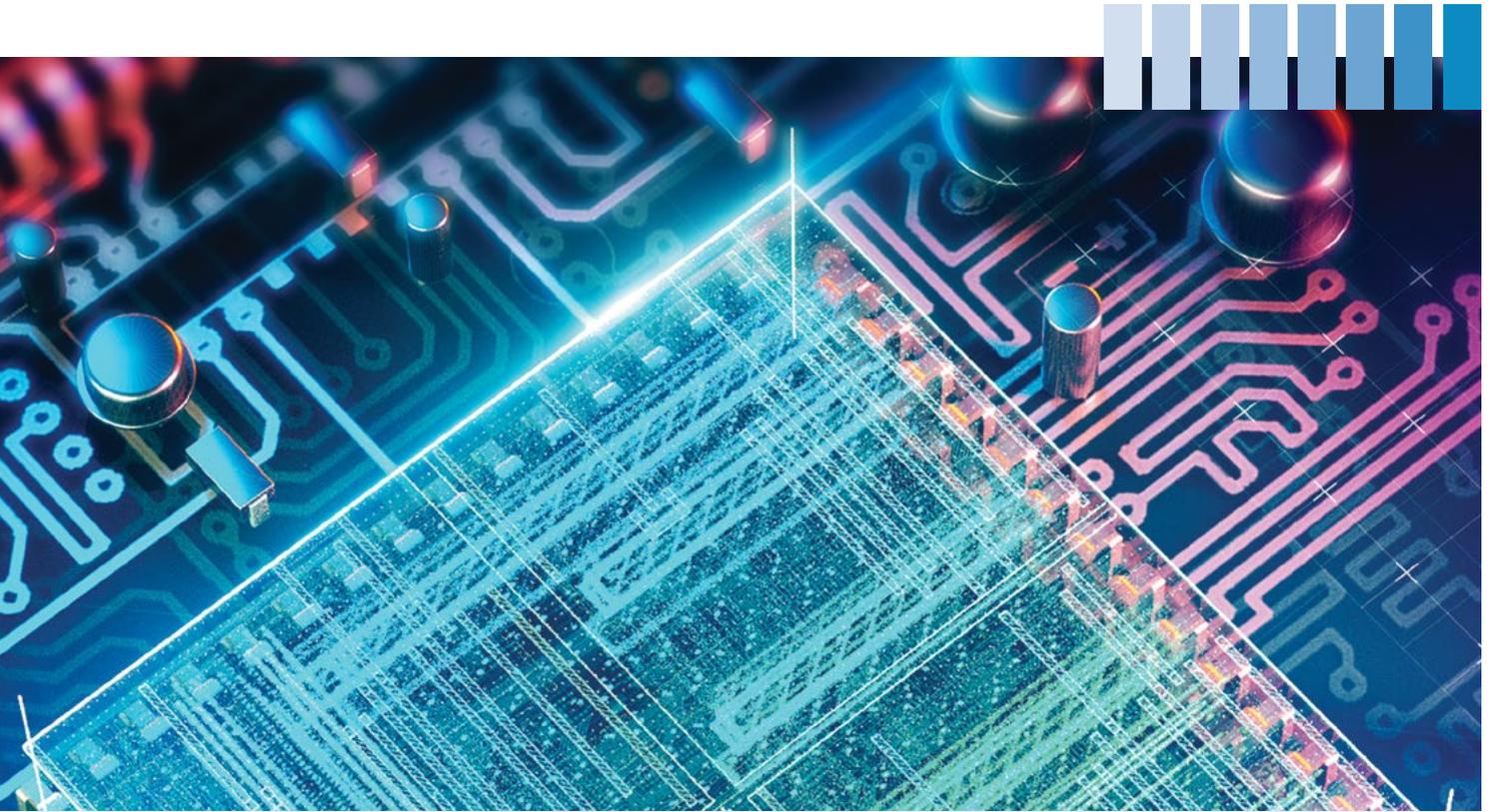
Companies such as Canberra-based QuintessenceLabs are tackling the security challenge to help companies become 'quantum safe', while seizing an important emerging business opportunity. QLabs, as the company is known, is at the heart of solving the security threat posed by quantum computers. The company has commercialised a device called a Quantum Random Number Generator, which promises to outwit cyber criminals by using encryption codes so random that not even a quantum computer could hack them without being detected.

QLabs's device, no bigger than a mobile phone, integrates into standard servers, generates truly random codes by measuring quantum tunnelling noise and converts the resulting signal to numbers. QLabs is also at the forefront of the development of quantum key distribution, protecting the exchange of keys using the laws of physics, and making it safe from even quantum computer attacks.

QLabs, formed in 2008 as a spin-off from the Australian National University in Canberra, has received numerous accolades. Its clients include over 30 organisations across the globe – including a dozen Fortune 500 companies and major Australian lender Westpac Banking Corp, which in 2017 bought a 16 per cent stake in the company and is using QLab's encryption capabilities to boost the security of its banking business.[36] Headquartered in Canberra, QLabs also has offices in Brisbane, and San Jose in California, with representation in Washington DC and London.

QuintessenceLabs was named a Technology Pioneer by the World Economic Forum in 2018, is a top 20 winner of the Westpac 200 Businesses of Tomorrow award, and won the SINET 16 award – ranking it as one of the top emerging innovation companies globally by the Security Innovation Network, which counts the US Department of Homeland Security and the Home Office in the United Kingdom as members.

36 QuintessenceLabs (2017), 'QuintessenceLabs Sees Additional Investment from Westpac Group to Strengthen Partnership'.
Available at: **https://www.quintessencelabs.com/press_release/quintessencelabs-additional-investment-westpac-group-cybersecurity/**.

Figure 35

Key stages of the cyber security research and innovation pipeline

◆ Limiting factor

Knowledge creation:
the origination of new ideas which are often based on prior research

Knowledge transfer:
identification and selection of knowledge for commercial application

Knowledge application:
development, trialing and refining of ideas that generate commercial applications

Lack of research focus

Low level of collaboration between researchers and industry

Difficulties accessing capital
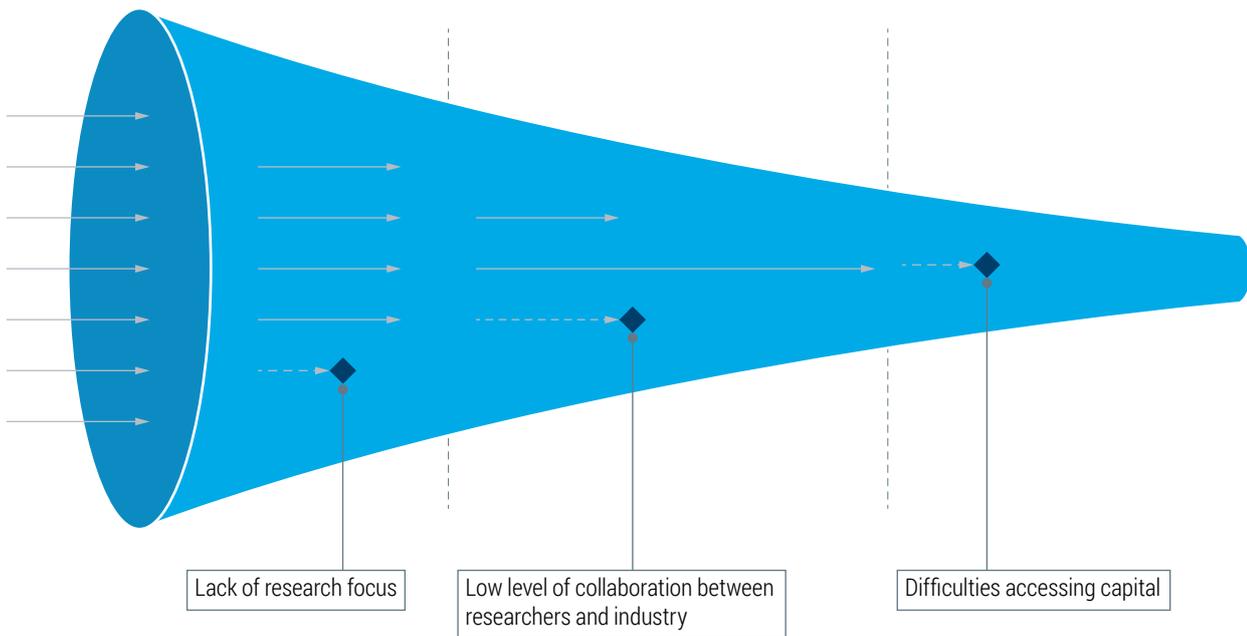
SOURCE: Innovation and Science Australia; AlphaBeta and McKinsey analysis

Australia needs to more effectively commercialise its cyber research. An often-cited criticism, underpinned by OECD data, is that Australia struggles to translate its academic strengths into marketable solutions.[37] The cyber security sector is no different. Several obstacles are blocking the innovation pipeline in cyber security and hampering the technological transition of high-quality research ideas into commercially viable products, as illustrated in Figure 35.

There is a lack of focus in existing research efforts

At present, university R&D in cyber security is comparatively small in scale and fragmented. The distribution of competitive ARC grants, as shown in Figure 36, indicates that public funding for cyber security research has been scattered across 16 universities over the past seven years, with no apparent effort to concentrate funding on a few national research flagships that could champion the knowledge creation in cyber security.

Even the Australian National University, which has so far received the highest individual amount of competitive research money in cyber security, still only attracted 14 per cent of the total ARC cyber security funding.[38] While there is value in diversity, a more concentrated funding approach would allow a select few universities to rapidly expand their cyber security research capabilities, and could help accelerate the creation of new ideas and spur the development of competitive technologies. The section *Grow an Australian cyber security ecosystem* in Chapter 4 identifies actions to help improve the focus of Australia's cyber security research.

37   Department of Industry, Innovation and Science (2017), 'Innovation, science and commercialisation at a glance'.
     Available at: https://industry.gov.au/Office-of-the-Chief-Economist/Publications/IndustryMonitor/section2.html.
38   Australia Research Council (2017), Grants Dataset. Available at: http://www.arc.gov.au/grants-dataset.

Figure 36

Distribution of competitive ARC research grants in cyber security

$, 2017–18   x Total funds (A$M)

The Australian National University	14%	2.4
University of Technology, Sydney	12%	2.1
The University of Melbourne	11%	1.8
Macquarie University	10%	1.7
RMIT University	10%	1.7
Queensland University of Technology	9%	1.6
Deakin University	6%	1.0
University of Wollongong	5%	0.9
Griffith University	5%	0.8
The University of Queensland	4%	0.7
The University of Newcastle	4%	0.7
University of the Sunshine Coast	2%	0.4
The University of Sydney	2%	0.4
The University of Adelaide	2%	0.3
The University of New South Wales	2%	0.3
Monash University	2%	0.3

Collaboration between industry and research is weak

A rich exchange between academia and industry is necessary to help researchers validate the practical applicability of their research and ensure research ideas get translated into practical applications. University scientists who cultivate a close collaboration with companies would find it easier to identify and select knowledge with commercial relevance. Businesses that collaborated on innovation were twice as likely to develop 10 or more innovations in the fiscal year 2015, Australian Government research shows.[39] Despite this, OECD data shows the ties between academia and industry in Australia are the weakest in the developed world: only 3 per cent of surveyed businesses in Australia collaborate with universities and other research

institutions – a sharp contrast to leading countries like Finland, where 69 per cent of large and 24 per cent of small companies work closely with external research organisations.[40]

The ties between academia and industry in Australia are the weakest in the developed world

As noted earlier, some of Australia's large companies in are acutely aware of the benefits of partnerships with local universities. For example, Commonwealth Bank of Australia has invested A$15 million to support researchers at UNSW who are part of the CQC[2]T network striving to build the world's first silicon-based quantum computer in Sydney (see Box 13 for details on CQC[2]T).[41]

39 Australian Government, Office of the Chief Economist (2016), *Australian Innovation System Report*.
    Available at: https://www.industry.gov.au/data-and-publications/australian-innovation-system-report/australian-innovation-system-report-2016.
40 OECD (2015), *Science, Technology and Industry Scoreboard*. Available at: http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/oecd-science-technology-and-industry-scoreboard-2015_sti_scoreboard-2015-en#page144.
41 Commonwealth Bank of Australia (2015), 'Commonwealth Bank Increases Support for Australian Leadership in Quantum Computing'.
    Available at: https://www.commbank.com.au/about-us/news/media-releases/2015/commonwealth-bank-increases-support-for-australian-leadership-in-quantum-computing.html.

3 THE CHALLENGE: AUSTRALIA NEEDS TO PLUG THE WORKFORCE GAP, REMOVE STARTUP BARRIERS, STRENGTHEN R&D, AND MEASURE GROWTH AND IMPACT

Quantum computing has potentially profound implications for cyber security, particularly through cryptography. The Commonwealth Bank of Australia's investment comes on top of Australian Government funding worth A$26 million for the CQC^{2}T, based at the University of New South Wales. An additional A$10 million of research funding for the project comes from Telstra, the nation's biggest telecommunications company, which has assigned its team of data scientists to work directly with University of New South Wales researchers. 'We can work together to put Australia at the forefront of global innovation,' said Telstra chief executive Andrew Penn in 2015, when the company announced the investment.[42]

Meanwhile, US technology company Cisco Systems has been instrumental in developing the Security Research Institute at Edith Cowan University in Western Australia.[44] Cisco further committed to invest US$15 million in a newly established Internet of Everything Innovation Centre with R&D facilities across Australia. The centre, which Cisco co-founded with Curtin University and Woodside Energy, is a space where customers, startups, open communities, researchers, entrepreneurs and technology enthusiasts can work and brainstorm on new ideas and technologies, including in cyber security.[45] Others working on deepening research and innovation links between large companies, universities and startups in Australia include Data61 within CSIRO (see Box 15) and financial technology hub Stone & Chalk.

Smaller industry participants, however, have been slower to tap into university expertise to develop new products and services. Interviews with a wide cross-section of local cyber security startups reveal that only two out of more than 22 industry particpants are currently working closely with universities.[46]

In interviews, industry participants cited several barriers to greater industry research collaboration in Australia. Some executives admit they lack experience in engaging universities to leverage their knowledge. Some also say that the different planning horizons limit their close collaboration with academics – companies tend to focus on their immediate, short-term needs, while basic research occurs over longer timeframes. Some company executives are reluctant to deepen their ties with researchers who they feel lack understanding of practical industry needs. Researchers, in contrast, said some industry customers have unrealistic expectations about what their business can gain from basic academic research. Lastly, both researchers and businesses agreed that negotiating intellectual property agreements with universities can be time-consuming and costly.

There is scope for a more effective collaboration of researchers and businesses

Chapter 4.1 (*Growing an Australian cyber security ecosystem*) makes several recommendations for actions that could help deepen the links between universities and industry, including offering work placements for postgraduate students.

42   Telstra (2015), 'Telstra announces plan to co-invest with Federal Government in silicon quantum computing'. Available at: https://exchange.telstra.com.au/2015/12/08/telstra-announces-plans-to-co-invest-with-federal-government-in-silicon-quantum-computing.

43   Macquarie University (2016), 'Optus Business and Macquarie University to establish new cyber security hub'. Available at: http://www.mq.edu.au/newsroom/2016/05/30/optus-business-and-macquarie-university-to-establish-new-cyber-security-hub/. See also the Optus Macquarie University Cyber Security Hub website at: http://www.mq.edu.au/about/about-the-university/offices-and-units/optus-macquarie-university-cyber-hub.

44   ECU Security Research Institute (2017), Director's notes. Available at: https://www.ecu.edu.au/corporate/template-bonito/craig-valli.html.

45   Cisco Systems (2015), 'Cisco Brings Internet of Everything Innovation Centre to Australia'. Available at: https://newsroom.cisco.com/press-release-content?articleId=1611789.

46   AlphaBeta/McKinsey (2017), Survey of Australian CIOs, CISOs and cyber security companies.

Box 15

Australia's digital dynamo: CSIRO's Data61

CSIRO's Data61 is the digital and data science arm of Australia's national science agency. Its purpose is to be the nation's most trusted research partner for impact-driven digital and data science. In doing so, it helps reinvent and create new industries for Australia. Today, Data61 is considered Australia's largest research and development facility of its kind. With 1,000 staff including 300 PhD students from 70 countries and a network of 30 university partners, it has sufficient scale and global reach to take on mission-driven, large-scale, multi-disciplinary research and commercialisation projects for Australia's government agencies, corporates and scalable growth companies.

The work is diverse. Scientists at Data61 have developed insect-like robots with legs whose sensors allow them to create a digital elevation map of an area or monitor unsafe and confined spaces such as aircraft wings, factories and mines. They have created software tools to help analysts predict the behaviour of bushfires to help emergency services better prepare for evacuations. They've also developed a world-first set of techniques to effectively 'vaccinate' algorithms against adversarial attacks.

Cyber security is a key research focus for Data61. For example, Data61's Trustworthy Systems Group has been recognised as world leaders in applying formal verification techniques to real-world systems – securing self-driving vehicles, autonomous drones, helicopters, satellites, land robots and trucks.

Other examples include:

- working with a major international airline manufacturer on Secure and Modular Internet of Things (SMIT) technologies, trailing lightweight authentication protocols and architectures for use in the manufacturer's supplier network;
- working with Australian Federal Police (AFP) on Data Airlock, which could enable data analytics in a secure enclave;
- working with a major European cyber security company and the RISC-V Foundation on critical system security; and
- continuing to collaborate with DARPA and Rockwell Collins on a joint Cyber Assured Systems Engineering (CASE) project.

Data61 closely collaborates with the defence and industry ecosystem. As part of a strategic partnership with Defence Science and Technology (DST) Group, they have 25 cyber security projects underway, which include research input from 14 universities within their network. Data61 is also leading as both an industry and research provider in the Cyber Security Cooperative Research Centre, joining 18 industry participants and 6 research partners.

A strong emphasis on research collaboration and increasing digital literacy underpins the Data61 model. The group connects academia, corporations, startups, governments, investors and entrepreneurs across the globe. For example, it has partnered with the Australian Institute of Company Directors and the Australian Graduate School of Management, run by the University of New South Wales, to deliver executive education courses on a range of topics such as cybersecurity, privacy and artificial intelligences.
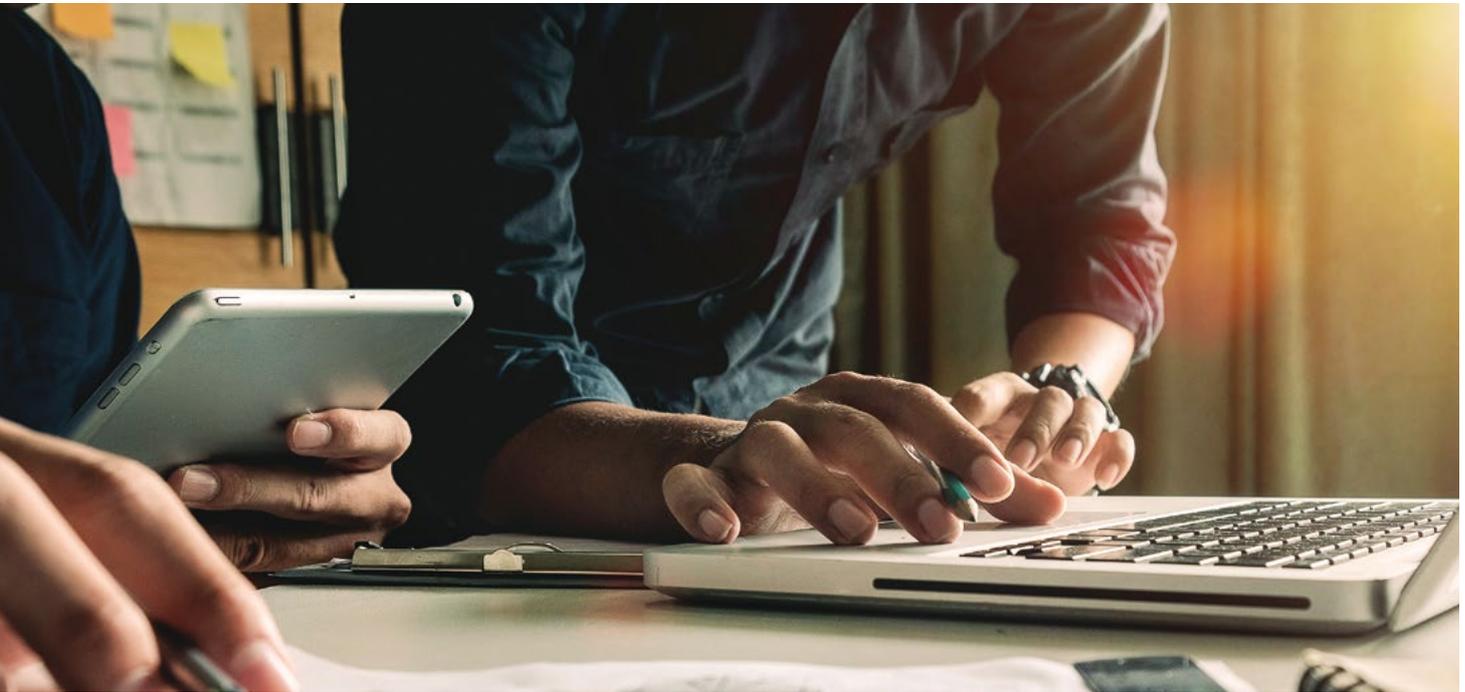
Access to capital to support innovation is limited

Venture capital funds investing in early-stage startups are currently scarce in Australia, noting some government assistance and incentives are available. This low availability blocks the country's innovation pipeline because startups are locked out from the high-risk capital they urgently need to turn promising ideas into competitive, real-life technologies.

OECD data, as shown in Figure 37 shows that, measured as a share of GDP, there is 10 times less early-stage venture capital available in Australia (0.01 per cent) than in the US (0.1 per cent) and almost 30 times less than in Israel (0.27 per cent). Both these countries are considered leaders in the global market for cyber security products.

> *'Cyber security is […] perceived as a risky and technically complex business. [Venture capital funds] in Australia are not interested in buying that extra complexity, particularly when they are in a medium-sized market that pushes them to be less specialised.'*
> Managing partner of large early-stage venture capital fund

Data compiled by the World Economic Forum, also shown in Figure 37 further highlight the difficulties Australian startups are facing when trying to tap venture capital funding.[47] On a scale from 1 (hard) to 7 (easy), Australian executives surveyed for the World Economic Forum's Global Competitiveness Index rate access to venture capital in Australia at 40th in the world, below the OECD average and well below our competitor nations.

This problem of access to early-stage venture capital funding is well-known and acknowledged in Australian Government assessments of the Australian innovation system.[48] Recent policy measures have attempted to address this through tax concessions. In 2016, the Australian Government also launched the CSIRO Innovation Fund, which aims to fill this funding gap by co-investing in spin-offs, startups and small to medium enterprises engaged in the commercialisation of early-stage innovations. CSIRO's science and technology innovation Accelerator, ON, also helps startups commercialise promising cyber security ideas.

47   World Economic Forum (2017), *The Global Competitiveness Report 2016–17*. Available at: http://reports.weforum.org/global-competitiveness-index.
48   Australian Government, Innovation and Science Australia (2016), *Performance Review of the Australian Innovation, Science and Research System 2016*. Available at: https://www.industry.gov.au/sites/default/files/2018-10/performance-review-of-the-australian-innovation-science-and-research-system-isa.pdf.

Figure 37

Quantity of early-stage venture capital funding

% of GDP, 2015

0.27	0.10	0.03	0.02	0.01
Israel	US	OECD average	UK	Australia
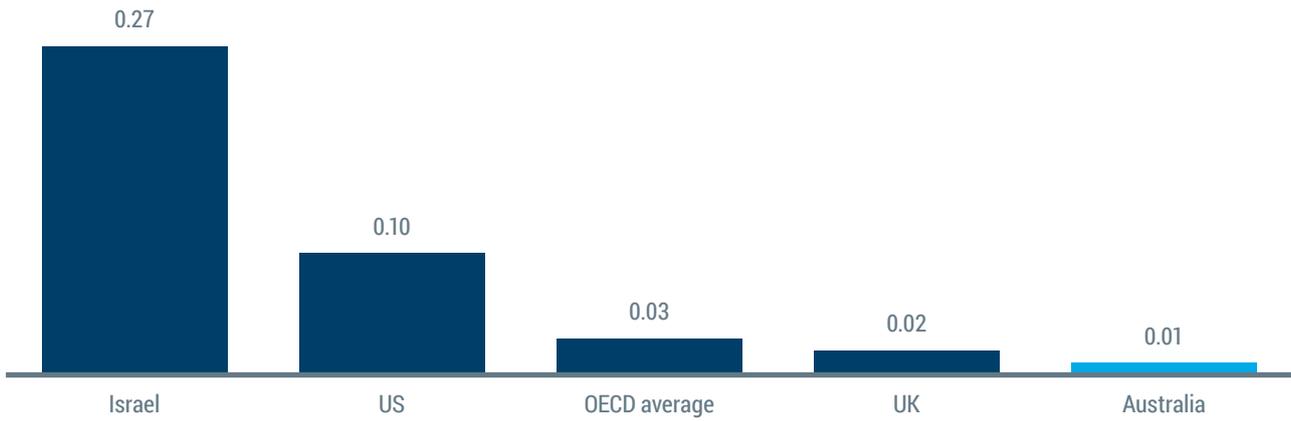
Venture capital availability

Index (1–7, 7 = best), 2015

(x) WEF competitiveness ranking

4.54	4.50	3.29	3.92	3.13
Israel	US	OECD average	UK	Australia
4	5		14	40
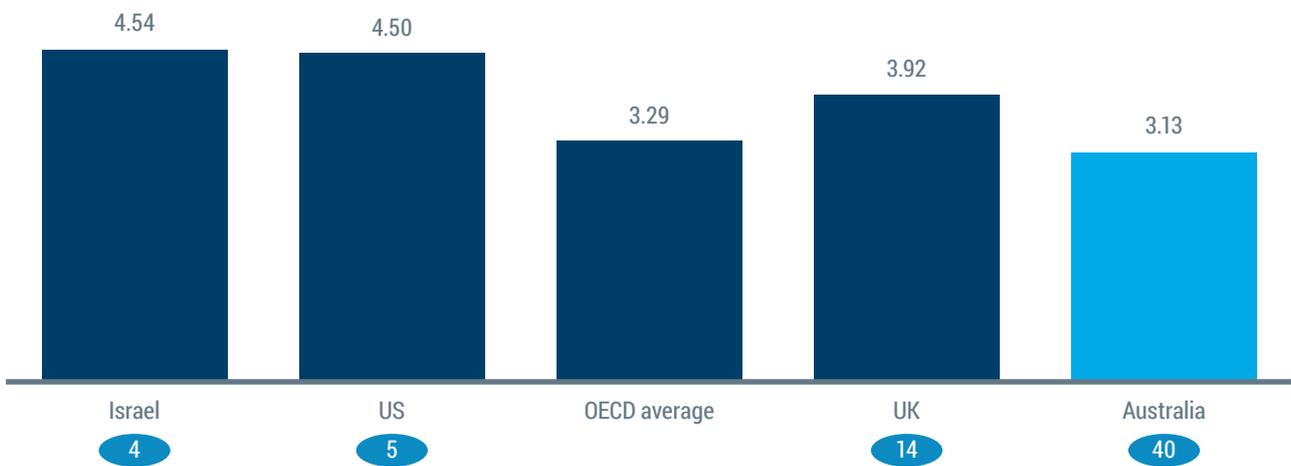
SOURCE: OECD indicators on Science and Technology; WEF 2015 Competitiveness Rankings; expert interviews; AlphaBeta and McKinsey analysis

'Pitching to early-stage [venture capital funds] in Australia was disheartening…They don't have much clarity and visibility around cyber, and their valuations were much lower than those of [Silicon] Valley investors.'
CEO of major Australian company

Cyber security startups, however, might face bigger obstacles than their peers because they offer complex, highly technical products. Most Australian venture capital funds are generalists by necessity because of the limited market size – as opposed to the US where there are several venture capital funds with expertise in cyber security (such as ForgePoint Capital and Paladin Capital). Interviews with Australian cyber security professionals indicate that local venture capital fund managers perceive the cyber security sector as complex and risky. Many are reluctant to invest because of a lack of expertise in this field, although this is starting to improve.

Local venture capital fund managers perceive the cyber security sector as complex and risky

Incubators and accelerators play an important role for Australia's cyber security ecosystem. They are part of the key infrastructure to foster business creation and innovation. While studies show that startups may be just as successful without that initial support, it is indisputable that accelerators and incubators help entrepreneurs learn a lot and improve their professional networks. There is also strong evidence that accelerators and incubators have a positive indirect impact, by 'serving as beacons' to unite a community and by increasing the diversity of interconnections in the ecosystem.[49] Focused incubators and accelerators that understand the cyber security ecosystem and its specific challenges should lead to a stronger performance of startups and their capacity to innovate.

Australia's first dedicated cyber security incubator, CyRise was launched in 2017. CyRise was borne out of a partnership between Dimension Data (now NTT) and Deakin University and with funding support from the Victorian Government's LaunchVic startup initiative. Australia could build on this great potential to develop an end-to-end network of cyber security infrastructure as a critical step towards a stronger domestic cyber security ecosystem.

'Cyber security startups work in the deep tech space. It therefore takes longer to build the right product and get traction, so they need more support than others.'
Scott Handsaker, CEO CyRise

Various approaches to overcome these issues are discussed in the section *Growing an Australian cyber security ecosystem* in Chapter 4, including familiarising new investor groups, such as superannuation funds, with investment opportunities in the local cyber security sector.

3.4 CYBER SECURITY COMPANIES' GROWTH AND EXPORT

Developing innovative products and services is crucial to building Australia's competitiveness in cyber security, but that alone is not enough to ensure our companies succeed and our industry develops. Companies need to be able to effectively sell their products and services into a domestic marketplace where they can build scale, confidence and capabilities. With that local base in place, they can more effectively take on the challenge of exporting to global markets and connecting with global value chains.

Barriers to growth for small cyber security companies in Australia

Interviews with buyers and sellers of cyber security solutions show companies need to overcome three main hurdles to successfully establish and grow their business – they need to understand their customers, gain trust, and get to scale.

---

49   See for example UNSW Business School (2016), *The role and performance of accelerators in the Australian startup ecosystem*. Available at: **http://unsworks.unsw.edu.au/fapi/datastream/unsworks:38003/bin8ca2e40f-1d69-4eb9-8d99-e332794b8f8f?view=true&xy=01**.

Figure 38

Most relevant factors for customers choosing a provider of cyber security products (software and hardware)

Relevance of each driver of competitiveness for purchasing decisions (0–10, 10= most relevant)   ■ Top 3 drivers by relevance

Drivers of competitiveness		Customers' assessment of relevance	Providers' perception of relevance to customers	Difference
Value differentiation	More effective technology	8.1	8.3	-0.2
	Better support	6.2	2.8	3.5
	Easier to use	2.0	3.9	-1.9
	Greater trust	4.8	6.7	-1.8
Cost competitiveness	Lower total price	4.2	2.2	2.0
	More flexible pricing model	2.6	1.7	0.9
Breadth of coverage and solutions	Broader presence	2.6	3.3	-0.7
	Wider range of solutions	2.6	4.4	-1.8

SOURCE: 2017 Survey of Australian CIO and CISO purchasing factors (N=21); expert interviews; AlphaBeta and McKinsey analysis

Cyber security companies often fail to understand their customers

The AlphaBeta/McKinsey survey of CIOs and CISOs and local cyber security providers indicates many Australian cyber security companies undervalue aspects of their offerings that are critical for local customers. This mismatch is most evident for customer support, according to the survey results shown in Figure 38. When purchasing products, customers consider support to be an essential component of their purchasing decision, while local companies are more focused on providing a user-friendly service. A greater understanding of, and focus on, local customer needs would help Australian cyber security companies grow.

Additional survey results shown in Figure 39 reveal that cyber security users have widely differing needs, depending on the nature of their businesses. Those most at risk of being targeted by cyber criminals, such as financial-services companies or defence agencies, are typically investing in large in-house cyber security teams and only seek external help to complement their own capabilities. When they do engage external service providers, they generally choose those offering the greatest trust, best support and most effective technology.

Figure 39

Most relevant factors for different customer segments choosing a cyber security product provider

Relevance of each driver of competitiveness for purchasing decisions (0–10, 10= most relevant)

Customer segment	High-end customers	Mid-market customers	... And the preferences of the integrating providers that serve the mid-market
Description	• Customers in sectors with a **high cyber security risk exposure** and maturity • They have capabilities to **fulfill most of their cyber security needs in-house**, and only look to the market for best-of-breed solutions	• Customers in sectors with a **mid to high cyber security risk exposure** and a lower cyber security maturity • These customers typically have **limited internal cyber security capabilities**, and look to cover most of their needs in the market	• Managed Security Service Providers (MSSP), which **develop their own products and services** and consolidate those of other companies into **one integrated offering**
Industry vertical examples	• Financial services • Defence	• Retail • Technology • Healthcare	• Telecommunications companies • IT managed service providers

Competitiveness preferences on products

	High-end customers	Mid-market customers	Integrating providers
More effective technology	10.0	7.6	7.0
Better support	6.1	5.8	7.7
Easier to use	1.1	1.9	3.7
Greater trust	5.6	4.3	5.5
Lower total price	3.6	4.6	4.2
More flexible pricing model	2.5	2.6	2.5
Broader presence	1.7	3.2	2.5
Wider range of solutions	2.8	3.3	0.3

SOURCE: 2017 Survey of Australian CIO and CISO purchasing factors (N=21); expert interviews; AlphaBeta and McKinsey analysis

Customers with a moderate risk exposure, such as retail and healthcare businesses, tend to outsource more of their security needs to external cyber security providers. These mid-market customers are most interested in acquiring the best technology and support when choosing a cyber security vendor. The survey shows they are also more cost-conscious than other customers in the market.

Cyber security companies also need to consider if their product or service might be better targeted to an integrator, such as a Managed Security Service Providers (MSSP), rather than

to end-user customers. MSSPs typically serve the needs of mid-market customers and usually bundle several products and services – from managed firewalls to vulnerability scanning and anti-virus services – into one integrated offering. Telecommunication companies are one example of MSSPs. Interviews suggest that MSSPs, on average, are most focused on offering their customers the best support, and least concerned about offering the widest range of solutions.

Box 16

Aussie cyber security innovator Datasec goes global with off device encryption

Printers are favourite targets for cyber criminals looking to gain access to a network or to intercept vital information. These devices store and process large amounts of information in order to print or scan documents – if an attacker gets a view of financial, HR or other sensitive documents, this can open the door to fraud and theft.

Datasec Solutions, a Melbourne based cyber security company, recognised this problem and built a solution in response, called Cryptix, focused on security and compliance issues at the point when organisations transmit private or business sensitive information.

Hewlett Packard (HP), a global US based company worth US$30 billion, was interested in how Cryptix solves the problem of secure printing without requiring IT administrators to navigate and install dozens of copies of software onto already busy devices. Cryptix utilises 'one-time pad' encryption technology, a digitised version of the same encryption technique used by spies and undercover agents for decades and the only universally accepted form of uncrackable encryption for secure messaging.

Importantly, Cryptix separates the control keys at the data level, which means that Cryptix does not provide a data 'honeypot' for hackers like other traditional file sharing services.

The partnership with HP marks a major win for Australian cyber security innovation and was achieved with the support of Austrade and AustCyber.

'With Cryptix, we've created something special in Australia that can quickly scale into a global business solution,' says Paul Waite, Solutions Director at Datasec. 'By working closely with HP, we aim to have 100,000 devices utilising Cryptix by the end of 2022, making the day-to-day operations of thousands of enterprises more secure.'

Cryptix is also fully compliant with a wide range of global regulations including Europe's General Data Protection Regulation, the United States' Health Insurance Portability and Accountability Act and the Australian Privacy Act, as well as being fully auditable. This means companies can track any scan and ensure maximum data governance.[50]

50   https://www8.hp.com/h20195/v2/GetPDF.aspx/4AA7-6385ENW.pdf.

New companies often lack the trust to gain anchor customers

To inform this Sector Competitiveness Plan, a range of local cyber security companies were analysed to understand which factors – including funding, R&D collaborations and industry regulation – are most important for their development and success. The results, shown in Figure 40 highlight that acquiring an 'anchor customer' is the most commonly cited success factor for Australian cyber security companies.

Anchor customers can add material value to a small business

They often have clout in an industry and can become a catalyst for demand by adding credibility to a startup and its new products. Their reputation often helps startups acquire further customers. They can also act as a strategic partner, provide access to fresh capital, and give feedback on how to improve a startup's offerings. Survey results show Australian cyber security companies most commonly relied on anchor customers from industry (relevant for approximately half the companies surveyed), while about one-quarter of the companies surveyed said a government contract was critical to their success.

Figure 40

Success factors for Australian cyber security firms*

% of firms for which the factor materially contributed to their success

		Software	Services
Collaboration	Collaboration with research institute	25	0
	Collaboration with an industry cluster	5	13
	Coordination from an industry body	0	0
Anchor customer	Government contract	23	25
	Industry customer	48	50
Funding	Govt research grant	0	0
	R&D tax incentive	29	13
	Australian VC funding	9	17
	International VC funding	24	17
	Private contract funding	19	17
	IPO	18	8
	Export assistance	5	0
Spin-off	University spin-off	0	0
	Industry spin-off	15	0
	Government spin-off	0	4
Regulation	Regulatory change	0	4
	Local content rules	0	13

*   Based on analysis of 22 Australian cyber security firms, with one or more success factors assigned to each firm

SOURCE: Interviews with company representatives; expert interviews; AlphaBeta and McKinsey analysis

However, acquiring an anchor customer is not easy and requires more than just a convincing product or service. A survey of CIOs and CISOs in leading Australian companies with the potential to act as anchor customers for cyber security companies reveals that trust is a crucial factor, particularly when selecting service providers.[51] And while buyers of cyber security products, such as antivirus software or firewalls, are generally most interested in buying the most effective technology, Figure 41 shows that finding a trustworthy producer still ranks as the third-most important driver for their purchasing decision.

This customer preference for dealing with a trusted vendor particularly affects the early-stage cyber security companies in Australia. In this market, which is dominated by well-established and reputable foreign competitors, many local startups lack the credibility needed to win an anchor customer.

'A common concern around local companies is that they need to go overseas to get their first sale…It's in fact an issue on the maturity of the local market…the fact that we don't realise that home-grown products can be world-class.'
CIO of an Australian bank

---

51   AlphaBeta/McKinsey (2017), 'Survey of Australian CIO and CISO purchasing factors'.

Figure 41

Most relevant purchasing factors for customers choosing a cyber security provider, 2017[*]

Relevance of each driver of competitiveness for purchasing decisions (0–10, 10= most relevant) ■ Top 3 drivers by relevance

		Products	Services
Value differentiation	More effective technology	8.1	5.2
	Better support	6.2	7.1
	Easier to use	2.0	2.1
	Greater trust	4.8	6.3
Cost competitiveness	Lower total price	4.2	5.3
	More flexible pricing model	2.6	2.6
Breadth of coverage and solutions	Broader presence	2.6	3.1
	Wider range of solutions	2.6	1.3
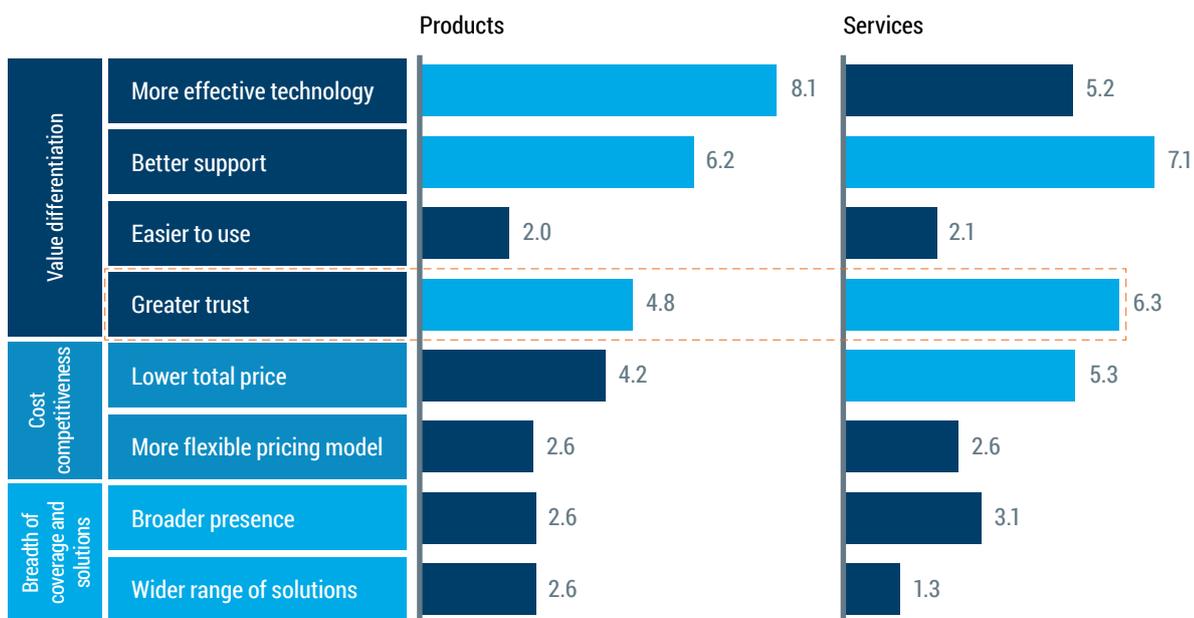
* CIOs and CISOs were asked to allocate 100 points across the drivers that are most relevant for them when assessing cyber security providers

SOURCE: 2017 Survey of Australian CIO and CISO purchasing factors (N=21); expert interviews; AlphaBeta and McKinsey analysis

Large potential customers may remain reluctant to engage if a company has no track record to indicate that a new product or service will deliver the promised outcome. Interviews with CISOs in Australia reveal many are hesitant to buy from smaller or newly established providers with no reputation, even if these companies offer technologically appealing products. Potential customers may also question the financial health of a cyber security startup and seek evidence that it will exist long enough to support its products and services well into the future.

In cyber security, a trust deficit can act as a stronger market barrier than in other industries. This is because buyers of cyber security products and services take a bigger risk with their purchases than buyers of other goods. As they invest in the protection of vast corporate IT networks with large amounts of sensitive data, they need a quality assurance and guarantee that what they buy will indeed shield them against cybercrime.

In cyber security, a trust deficit can act as a stronger market barrier than in other industries

One way for companies to overcome the lack of trust is to use one of several certification and accreditation programs available in Australia (see Box 17 for further details). Another, less obvious way to overcome local market barriers is to expand overseas. Some local cyber security companies have found it easier to penetrate the Australian market after acquiring an international customer first. In interviews, company executives said the fact that foreign customers can help increase the perceived trustworthiness of Australian cyber security companies illustrates the widespread risk aversion in the local market.

The section *Growing an Australian cyber security ecosystem* in Chapter 4 outlines actions that can assist cyber security startups in their search for anchor customers, including showcasing Australian cyber security products and services and coaching to help startups mature their business operations.

Box 17

ASD accreditation programs for Australian cyber security companies

The Australian Signals Directorate (ASD), a statutory agency within the Australian Government's Defence portfolio that is also responsible for the Australian Cyber Security Centre (ACSC), evaluates and certifies ICT products and services that meet the high-level security standards of government agencies. This can be important for any cyber security company wishing to win a government agency as customer. ASD currently has several certification and accreditation schemes that businesses can participate in.

- **Australasian Information Security Evaluation Program (AISEP)** – assesses whether ICT security products and systems work effectively and to specification, and if they show any exploitable vulnerabilities. Products and systems that pass assessment are added to a Certified Products List (CPL) on the Common Criteria website, which approves their use by Australian and New Zealand government agencies and certifies them against international standards.

- **The ASD Cryptographic Evaluation (ACE)** – analyses products to determine whether their security architecture and cryptographic algorithms have been implemented correctly and are strong enough for the product's intended use.

- **The High Assurance Evaluation Program** – involves rigorous analysis and testing to search for any security vulnerabilities in a product.

  – Products that have been evaluated via the ACE program or the High Assurance Evaluation Program go onto the Evaluated Products List (EPL), which provides a 'consumer guide' for each product containing a brief description of the product, the scope of the evaluation and recommendations for secure product usage.

- **ASD Certified Services** – tests and certifies the effectiveness of gateway services and cloud services.

- **Information Security Registered Assessors Program (IRAP)** – trains and accredits individual cyber security professionals to assess organisations' security compliance and highlight information security risks, with a focus on compliance with Australian Government information security standards and requirements.

Procurement processes favour larger, established companies

Strict procurement rules oblige many government agencies and private-sector companies to engage only cyber security providers with a proven track record of fulfilling complex and sizeable security tasks. These internal procedures typically work in favour of large cyber security companies, while startups frequently miss out. Many small, emerging cyber security companies lack the resources to deliver large-scale projects, particularly when they cover multiple product and service areas as government contracts often do. Government agencies often search for providers who are capable of meeting a variety of security and other ICT needs at once – a tendency clearly reflected in the scope of government contracts, which are among the most valuable in the market.

An analysis of Australian Government tender agreements for the provision of cyber security services over the past decade, illustrated in Figure 42 shows that just one-quarter of all government contracts made up almost 87 per cent, or A$274 million, of the entire government spending on cyber security contractors over that period. Yet, only 8 per cent of these high-value government contracts were concluded with Australian grown and owned companies, as most are still too small to effectively compete against large foreign rivals in a government tendering process.

Missing out on the large-scale contracts commonly offered by Australian Government agencies – a median size of A$300,000 for the top quarter of contracts – is a significant barrier to entry for smaller Australian cyber security providers. In fact, large-value contracts are seen as the most important market hurdle for startups globally.

Figure 42

Government cyber security-specific contracts*, 2007–17
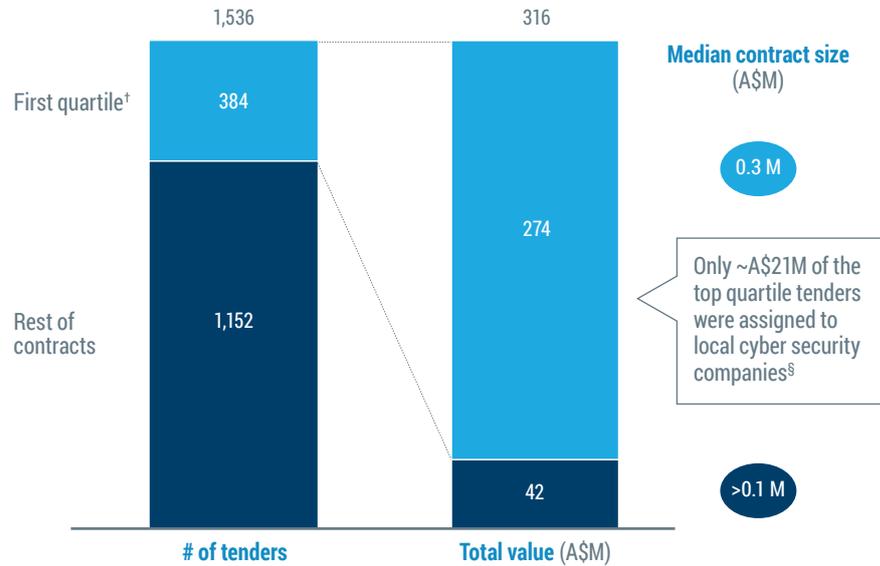
* Analysis of contracts specifically marked for cyber security or related activities; does not include spend that might be bundled into broader IT agreements

† Based on total contract value

§ Excludes companies that were founded in Australia and acquired by foreign companies (e.g., UXC and Saltbush Consulting)

SOURCE: AusTender keyword search; press search; AlphaBeta and McKinsey analysis

'Big organisations tend to hire big organisations.' CIO of an Australian bank

Research shows, for example, that the share of small and medium-sized companies securing government tenders in European Union countries rapidly declines once the overall contract value rises above A$150,000.[52] Tender processes could be made more accessible if governments divided their contracts into smaller parcels. Rather than contracting a few very large cyber security service providers, they could allow many small companies to service different aspects of their security needs. Given that purchasing from more providers could also make systems more complex and less integrated, any move to smaller contracts would need to be properly weighed against such potential complications.

Tender processes could be made more accessible if governments divided their contracts into smaller parcels

Other aspects of the public procurement process are also hindering cyber security startups from working more closely with government. Public agencies usually appoint a panel of suppliers for products and services they regularly acquire, referred to as Standing Offer Notices. These suppliers are pre-approved to do business with the government for a period of several years. While this offers convenience for procurement officers, it limits opportunities for new entrants. One example is the panel for 'Consultancy and Business Services', which comprises 170 suppliers and has been used to procure some cyber security-related contracts.[53] The current panel was appointed in 2013, and there will be no new opportunities to join this panel until it expires in 2019.

52 PwC/ICF GHK/Ecorys (2014), SMEs' access to public procurement markets and aggregation of demand in the EU.
   Available at: **https://ec.europa.eu/docsroom/documents/15459/attachments/1/translations/en/renditions/native**.
53 **https://www.tenders.gov.au/?event=public.son.view&SONUUID=9EF01E95-D79C-2555-7DB88D34335030ED**.

3 THE CHALLENGE: AUSTRALIA NEEDS TO PLUG THE WORKFORCE GAP, REMOVE STARTUP BARRIERS, STRENGTHEN R&D, AND MEASURE GROWTH AND IMPACT

The Australian Government is trying to remove barriers to entry. Recently, it has added new features to its 'Digital Marketplace' – an online platform for buyers and sellers of various ICT products and services. It has opened up the Digital Marketplace to cyber security businesses, making it easier for them to work with Australian Government agencies. The Digital Marketplace uses a strict selection process for companies wishing to use the platform for their offerings. Similarly, cyber security services companies must demonstrate certain abilities and experiences before they can join the Digital Marketplace.[54]

Importantly, the Digital Marketplace could also provide cyber security companies with access to state and local government buyers. In addition to launching its own marketplace for the cloud,[55] the New South Wales government has already announced that the Marketplace complies with its procurement policies, and it will begin purchasing some ICT services through the new platform.[56] Some local governments have also joined as registered buyers. A uniform set of procurement requirements to access buyers at all levels of government will significantly reduce compliance costs for companies.

Many of these issues in public sector procurement are also common to private sector procurement processes, which are often deliberately designed to weed out startups and smaller companies through narrow evaluation and review criteria. The preference to work with larger players is particularly strong in cyber security, which affects highly sensitive aspects of the business. Lengthy procurement processes, usually lasting between three and six months, can additionally deter smaller providers.

Simplifying procurement procedures in the public and private sector would remove some of the substantial hurdles that cyber security startups are facing. Section *Grow an Australian cyber security ecosystem* in Chapter 4 has more details on actions to address this issue.

Cyber security companies traditionally struggle to access export markets

An analysis of the geographical spread of Australian cyber security companies reveals significant scope for the sector to export its products and services and connect to global value chains. While many Australian hardware and software providers are already engaging with global customers, most services companies in the Australian cyber security sector have not yet developed an export capability. In fact, Figure 43 reveals that only 12 per cent of Australian cyber security services companies surveyed have customers outside Australia, although anecdotal reports suggest this is growing.

12%
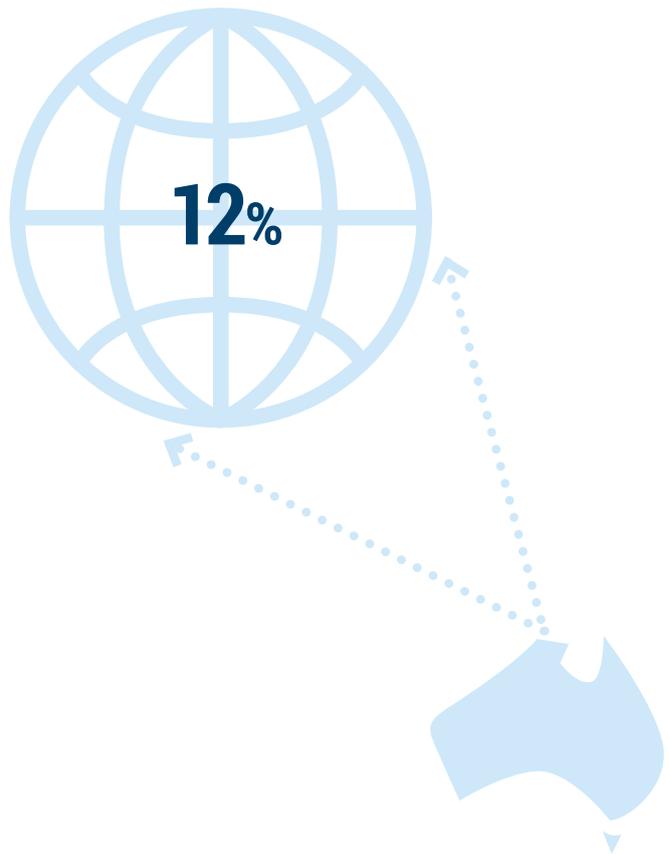
54   For a detailed list of criteria see: **https://marketplace.service.gov.au/assessment-criteria#cyber**.

55   **https://www.digital.nsw.gov.au/article/introducing-buynsw**.

56   New South Wales Government Department of Finance, Services and Innovation (2016), 'NSW Government the first to collaborate with the DTO's new Digital Marketplace'. Available at: **https://www.finance.nsw.gov.au/about-us/media-releases/nsw-government-first-collaborate-dto%E2%80%99s-new-digital-marketplace**.

Figure 43

Overseas activities of Australian cyber security firms

% of identified firms, n=41, 2017
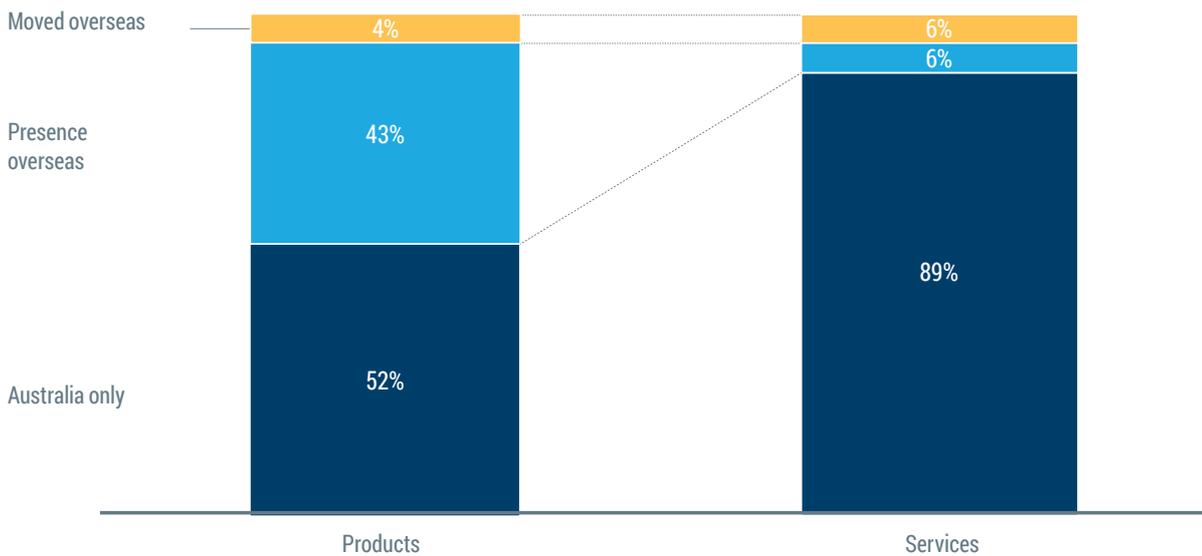
Note: Shares may not sum to 100% due to rounding
SOURCE: Expert interviews; press search; AlphaBeta and McKinsey analysis

Not all cyber security services are equally exportable. Education is unique because it is relatively easy for a cyber security training provider to bring individual students to Australia to study. A data analytics company, however, might struggle to export its services due to country-specific laws around data privacy. Service providers offering advice and support on compliance issues might also find it difficult to export their work, as they require a deep knowledge of local regulations.

Some services exports require a local operating base in another country. Others can be delivered remotely, meaning jobs created are predominantly in Australia. The way companies design their service offerings can have a major impact on their exportability, and some Australian cyber security companies may need more support and guidance to develop the most exportable service possible. Still, some service providers may not yet have the staff,

expertise and resources needed to serve customers abroad. In interviews, several cyber security services companies indicated that exporting is not a priority for them, because they already struggle to recruit enough cyber security professionals to meet strong domestic demand.

Chapter 4 lists several strategies that could help overcome some of the common export issues Australian cyber security companies are facing. Examples include intensifying Australia's marketing presence for cyber security in key target markets and analysing remote delivery models for Australia's existing services strengths.

3.5 MEASURING GROWTH AND IMPACT

A clear view of the state and size of the cyber security sector is essential for sustained growth. The lack of trusted sector measures and data can hinder cyber security's growth trajectory. Good policy and future investments are contingent upon policymakers, entrepreneurs and investors having a clear picture of the sector on which to make informed decisions. Without a solid fact-base about the local sector's demographics and performance, policymakers may fail to identify factors that both contribute to and prevent growth and productivity. Investors who cannot assess potential commercial opportunities in the sector due to a paucity of information will be unable to calibrate their investments in the sector. A lack of in-depth understanding of the sector's value to the growth and outcomes of the economy overall, hampers the nation's ability to assess with sophistication the global competitiveness of all sectors.

There are two main reasons why measurement of the sector has proved so challenging. Firstly, there is a dearth of quality data as new and emerging sectors like cyber security are not captured by standard government industry and occupation codes – nor are frameworks and codes particularly mature around representations of intangible assets of which cyber security is majority comprised. This is coupled with the fact that firms tend to be very reticent in disclosing any information related to security, whether it be their level of protection or their experiences of cyber threats. Secondly, the nature of the sector makes it difficult to segment and analyse as it consists of both a discrete vertical sector that sells cyber security goods and services, combined with a horizontal cyber security function across the economy.

It is also important to grow our understanding of the role of cyber security in the broader economy. This can best be understood through three elements, which have both direct and indirect considerations:

(1) the *risk* of malicious cyber incidents and cyber attacks;

(2) the *protection* offered by cyber security; and

(3) the *benefits* of that protection. Individuals and organisations can manage cyber risk with protective measures that include software, behaviours and services.

Understanding the cyber risk environment is vital as it directly informs firms about the level of protection required. Gauging overall investments in cyber defences establishes benchmarks and a basis for firms to judge whether their levels of protection are comparable to their peers.

However, cyber security does not only mitigate risk – its products and services, as well as its innovation and investment cycles and advances in workforce growth and maturity, also fuel economic growth. Improved trust in the digital environment accelerates digitisation across the economy and lowers barriers to information exchange, resulting in productivity gains and incentives to pursue innovative ideas. In this way, cyber security serves as an enabler of growth and prosperity especially as the economy continues to digitise.

Improving measurement of both the sector itself, as well as the its broader impact, is vital. In the short-term, there should be an annually updated robust estimation of the sector's growth and development. In the long-term, cyber security should be incorporated into the Australian Bureau of Statistics' (ABS) regular measurement program alongside other technology focused sectors. Existing measurements of cyber security risk and protection by government agencies should be enhanced, and economic analysis undertaken to better understand the broader benefits that cyber investments generate.

The Australian cyber security sector is not being adequately measured

Although there are broad estimates of sector revenue and spending on cyber security goods and services, such as those presented in this Sector Competitiveness Plan. There are no detailed, systematic measurements of the Australian cyber security sector yet.

Other sectors rely on the ABS, which undertakes regular measurements of Australian industries and occupations. These regular ABS measurements result in essential economic data, such as the national accounts, and form the authoritative description of Australia's economy. However, the ABS' industry measurements are based on the Australian and New Zealand Standard Industrial Classification (ANZSIC), which does not recognise cyber security; instead, the cyber security sector's activities span several ANZSIC codes, with a mix of computer systems design and professional services (Figure 44). For occupations, the ABS relies on its Australian and New Zealand Standard Occupation Code (ANZSCO), which does refer to cyber security in a single category ('ICT Security Specialist'). Besides the fact that one occupation code is insufficient to capture the range and variation of cyber security roles, the ICT Security Specialist designation is at the lowest possible level in the classification system, and most ABS measurements are not reported with that degree of granularity.

Figure 44

Current industry and occupation classification standards for cyber security

ANZSIC industrial codes relevant to cyber security

58	**Telecommunications Services**	
	580	Telecommunications Services
59	**Internet Service Providers, Web Search Portals and Data Processing Services**	
	591	Internet Service Providers and Web Search Portals
	592	Data Processing, Web Hosting and Electronic Information Storage Services
69	**Professional, Scientific and Technical Services (Except Computer System Design and Related Services)**	
	691	Scientific Research Services
	699	Other Professional, Scientific and Technical Services
70	**Computer System Design and Related Services**	
	700	Computer System Design and Related Services

ANZSCO occupation codes relevant to cyber security

13	**Specialist Managers**			
	135	ICT Managers		
26	**ICT Professionals**			
	261	Business and Systems Analysts, and Programmers		
	262	Database and Systems Administrators, and ICT Security Specialists		
		2621	Database and Systems Administrators and ICT Security Specialists	
			262112	**ICT Security Specialist**
	263	ICT Network and Support Professionals		
31	**Engineering, ICT and Science Technicians**			
	313	ICT and Telecommunications Technicians		

This problem of poor sector economic data is not unique to Australia. Currently, there are no robust and repeatable government measurements of the cyber security sector in any country, meaning that its economic characteristics are poorly understood. This is not because of ambivalence towards cyber security. Most developed economies have launched detailed national cyber security strategies, but neither their statistical agencies or governmental departments are carrying out sector measurement programs. The exception is the United Kingdom, where two government departments – one concerning business and industry and the other digital affairs – commissioned sectoral analyses in 2013 and 2018 respectively.[62]

57   UK Dept for Business, Innovation, and Skills (now known as Business, Energy, and Industrial Strategy) (2013) <u>Competitive Analysis of the UK Cyber Security Sector</u>. Available at: <u>https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/259500/bis-13-1231-competitive-analysis-of-the-uk-cyber-security-sector.pdf</u>. UK Department for Digital, Culture, Media, & Sport (2018) <u>Cyber Security Sectoral Analysis and Deep-Dive Review</u>. Available at: <u>https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/751406/UK_Cyber_Sector_Report_-_June_2018.pdf</u>.

Several aspects of sector development need to be measured

There are several dimensions to consider when measuring the cyber security sector. These can be organised according to descriptive and performance measures (Figure 45). Descriptive measures deal with basic, fundamental facts about a sector such as the number of firms operating, employment, and revenue earned. Governments can use this information to adjust policies aimed at developing the sector, such as planning for the sector's employment and skills needs. More refined descriptors such as the age and size distribution of firms and workforce demographics are useful in answering more specific questions on sector maturity, the flow of talent into the workforce and workforce equity.

These basic descriptors provide the foundation for more complex performance measures to determine a sector's overall contribution to the national economy. Key performance measures include gross value added (GVA), which directly informs national GDP calculations, and the value of exports from the sector. This information allows investors to calibrate their investments in the sector, and helps government understand the economic value of the sector and the impact of industry policy settings and efforts over time.

Figure 45

Application of typical sector measurements to cyber security

Sector measurements		Metric	Importance
Descriptive measures	Firm profiles	• No. of firms	• Crucial for effective policy development
		• Age and size of firms	• Informs employment and skills needs, which is critical to skills policy
	Employment	• FTEs	
		• Workforce demographics	
	Revenue	• Revenue	
Performance measures	Value added	• GVA	• Helps investors calibrate their investment decisions
	Export value	• Export value	• Government is best placed to assess whether sector performance and export contribution has improved over time

Several possible approaches could be used to better measure the sector

While the optimal measurement of cyber security as a sector would be through its inclusion in the Australia and New Zealand Industrial Classification (ANZSIC), revisions of industry classification occur infrequently and are complex and costly. Statistical agencies are rightly cautious to revise their standards because any changes affect the continuity of historical economic data. ANZSIC, for example, was first released in 1993 as a replacement for the Australian Standard Industrial Classification and has only been revised once since then, in 2006. It does not capture the digital economy well. For example, it splits the ICT sector into two groups: an ICT group and a professional services group.[58]

Statistical agencies have developed an alternative approach to measuring sectors which are not included as industries in national accounts. These are called satellite accounts and have been adopted for several industries. The most notable example is tourism, which is not a sector in ANZSIC because it consists of the provision of different types of goods and services – accommodation, food and beverage and souvenirs – to a common customer, a tourist. The ABS has published an annual satellite account for tourism in Australia since 2000–01. Satellite accounts have also been tested or used in various jurisdictions for transport, the environment and households.

The ABS could address the problem of cyber security measurement in the same way by assigning the sector its own satellite account or more ambitiously, as a component of an account that encompasses the digital economy. The ABS has taken some steps towards using these approaches for the ICT sector. It produced an ICT satellite account for 2002–03, but this was discontinued.[59] More recently, the ABS tested the application of an OECD/BEA framework for measuring the digital economy.[60] However, neither of these approaches explicitly included the cyber security sector.

Introducing a cyber security or digital economy satellite account would take time. The robust and rigorous approach of ABS studies necessitates a long measurement period and requires significant funding, which may be challenging to secure. If these feasibility challenges can be overcome, such a study would be highly credible, comparable to other sectors in the country and future measurements in other jurisdictions, and easily repeatable if it is treated as other satellite accounts.

Given the long lead time likely to develop a satellite account for cyber security, it will likely be necessary to implement an interim solution. Several private sector organisations have attempted to measure countries' cyber security sectors. These private sector studies tended to choose from five main data sources to estimate descriptive and performance measures (Figure 46). These data sources each have benefits and drawbacks. For example, detailed government records of firms and proprietary databases would offer a great deal of insight into the sector, but these are difficult to access. In contrast, readily available public data sources can lack relevant and detailed information. The most successful of these measurements used multiple sources of data to compensate for the lack of government data assets such as tax records or granular national accounts data.

Two approaches to sector measurement are proposed in Chapter 4. The first is a long-term plan to incorporate the cyber security sector into the ABS' regular measurement program, either as part of a revamped industry classification code or as a satellite measurement account alongside other technology sectors. The second is a short-term plan to plug the knowledge gap through an independent measurement of the sector drawing on various available data sources.

58   Australian Computer Society (2015) Submission to the ABS and Department of Communications for the Review of ICT Statistics. Available at: https://www.acs.org.au/content/dam/acs/acs-public-policy/ACS%20Submission%20to%20the%20ABS%20Review%20of%20ICT%20Statistics%20-%20February%202015.pdf.
59   ABS (2006) Australian National Accounts: Information and Communications Technology Satellite Account, 2002-3. Available at: https://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/5259.0Main+Features12002-03?OpenDocument.
60   ABS (2019) Measuring Digital Activities in the Australian Economy. Available at: http://www.abs.gov.au/websitedbs/d3310114.nsf/home/abs+chief+economist+-+full+paper+of+measuring+digital+activities+in+the+australian+economy.

Figure 46

Assessment of potential data sources for sector measurement

Legend: **High** (grey) | **Medium** (blue) | **Low** (dark navy)

	Public data	Survey	Interview	Government records of businesses	Proprietary private database
Examples	Published annual corporate reports, news stories, research studies	Survey to cyber security providers	Interviewing industry leaders and experts	Data from a government companies register, tax records	Data bases from Orbis, IBISWorld, Osiris
Benefits	Easy to access	Easy to scale	Insightful	Comprehensiveness	Insightful
Challenges	Limited insight	Difficult to verify. Difficult to obtain representative sample	Time consuming, expensive, difficult to scale	Difficult to access	Difficult to access
Robustness	Low	Medium	Medium	High	High
Affordability	High	Medium	Low	Depends on user, low if estimator is government	Low
Reason for assessment	• The quality of public data varies from one jurisdiction to the next • Public data offers information that is general or specific to large firms so estimates based on public data will have to rely strongly on assumptions	• Survey data is common in studies on the sector but surveys are often targeted at customers of cyber security to assess spending on the sector, instead of being targeted at the sector itself to assess revenue	• Interviews can provide great insight but are laborious and difficult to scale across an entire sector, which means that estimates rely on some strong assumptions	• Generally, Australia has high-quality government records that could be used for sector measurement, though there is a significant delay to access this information • Difficult to access for non-government investigators	• Typically provide rich and high-quality data on firms, including private companies, with sufficient detail to calculate complex metrics e.g. GVA • High cost to access and can be time consuming to use

Cyber security's impact on the broader economy can be understood through three elements – risks, protection and benefits

Studying the key indicators and descriptors of the sector is only half of the measurement challenge. Another important challenge to tackle is improving our understanding of cyber security's role and impact on the broader Australian economy. This can be achieved by focusing on the elements of risk, protection and benefits. Firms and people respond to the *risk* of security breaches through implementing *protection* measures, which then confer *benefits*. Assessing each of these three elements of cyber security in a credible way is essential to understand how cyber security interacts with the broader economy (see Figure 47).

Risk is a measure of the degree to which organisations, individuals and the economy are vulnerable to attacks, as well as the consequences of a successful breach. This includes the financial costs of detection, data recovery, investigation, network restoration, training and customer or supplier retention. Damage to an organisation's reputation is also costly and for government and national institutions, security compromises often have political implications at home and abroad.

Protection describes organisations' use of up-to-date protective technologies and services and whether such protection extends to the entire set of a firm's digital assets. These components are often summarised and reported as readiness indices which assess the overall level of protection. Cost of protection is also a key aspect when assessing protection – this includes the cost of products and services, as well as wages of in-house cyber security staff.

Cyber security benefits organisations in two ways. The first type of benefits are the losses avoided as a result of thwarted attacks. This benefit can be quantified according to the difference in the cost of offsetting cyber risk compared to the cost of a successful attack. The second type of benefits are those resulting from the protective or enabling effects of cyber security on economic sources of value. For example, digital activities such as e-commerce, online banking, and cloud computing are increasingly impossible without adequate cyber protection.

A range of risk measurements have been developed internationally, focusing on the costs of breaches and levels of cyber risk

Risk has typically been measured by quantifying the cost of a cyber breach to an organisation, or by assessing the incidence of cyber breaches for organisations or countries. While some governments have undertaken such assessments, limited government activity in risk measurement has prompted several private sector organisations – cyber security vendors in particular – to take a leading role. Given the commercial interest of vendors in emphasising the costs of inaction, this has raised concerns about the credibility and reliability of their risk measurements (see Box 18).

Two standout studies on risk were performed or commissioned by national governments. Statistics Canada, Canada's national statistics agency, surveyed over 7,000 private firms on the incidence of cyber breaches as part of a broader study on cybercrime (Canadian Survey of Cyber Security and Cybercrime).[61] In the United Kingdom, the Department for Digital, Culture, Media & Sport conducted an in-depth survey of more than 2,000 private firms and charities, asking about the number and cost of breaches, followed up by 50 interviews to add depth to the findings.[62] In both these cases, the substantial sample size combined with a well-designed survey and robust interpretation resulted in more meaningful and interesting findings compared to private sector studies, which focus on estimating the average cost of a breach from a limited survey sample.

---

61 Statistics Canada (2017) **Cyber Security and Cybercrime in Canada**. Available at: **https://www150.statcan.gc.ca/n1/pub/71-607-x/71-607-x2018007-eng.htm**.
62 UK Department for Digital, Culture, Media & Sport (2018) **Cyber Security Breaches Survey**. Available at: **https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018**.

3 THE CHALLENGE: AUSTRALIA NEEDS TO PLUG THE WORKFORCE GAP, REMOVE STARTUP BARRIERS, STRENGTHEN R&D, AND MEASURE GROWTH AND IMPACT

Figure 47

Measuring cyber security's impact on the economy

	Organisations and individuals respond to the risk of security breaches through... Risk	...instituting protective measures... Protection	...which confer benefits Benefits
Significance	• For organisations and individuals, measuring risk is essential for firms to understand the threats they face and calibrate suitable responses • An overview of the risk environment informs policy settings for government and estimates the potential harm cyber crime can inflict on the economy	• Understanding readiness and investments in protection by peers helps organisations to benchmark their own investments • It can also help governments to assess national readiness, and to identify weak spots in particular industries or geographies that may require government intervention	• Organisations and individuals need to measure benefits to assess their return on investments in protection, in the form of avoided losses • For government, measuring benefits accrued to firms, the local sector, and the wider economy will allow it to better understand a complex cyber ecosystem to inform policy and calibrate investment
Analytical components	• The **vulnerability to** cyber security attacks, which can be measured according to: – The pervasiveness of threats, in terms of the incidences of attacks, the proliferation of new threats, and accessibility to attack tools – Extent of risk exposure – Extent of digitisation • The **impact of cyber breaches** can be measured according to: – The type of impact a breach has in terms of data loss, system corruption, website defacement, service downtime, and loss of service – The financial costs of a breach in terms of detection, data recovery, investigation, and restoration	• The **level of cyber security protection** can be measured according to: – Accessibility and uptake of protection – The extent of a firm's or economy's digital assets that is protected – Readiness index reflecting cyber security protections in place • The **cost of cyber security protection** in the form of cyber security goods and services, which can be measured by: – Spend on the purchase of cyber security products and services by organisations and individuals – Spend on wages of cyber security staff	• Investment in cyber security capabilities returns **direct benefits in the form of avoided losses** for firms • As firms protect themselves, demand for cyber products and services increases which **grows the cyber sector** • Economy-wide benefits can be modelled according to counterfactuals: what **value is gained in the case of better investment** and lost in the case of poorer investments than current BAU • Investment in cyber security capabilities has important **spill-over effects**: – Increased trust and collaboration amongst firms in a network – Enhanced global competitiveness – Sovereign capability – 'Herd immunity', where a secure ecosystem shields unprotected firms

Box 18

How much does a cyber attack cost victims?

Overseas, one of the mostly commonly used cyber risk measures is estimating the cost of a successful malicious cyber incident. Studies of this measure attempt to motivate investment in appropriate levels of cyber protection by reporting the costs of inaction. However, there is a lack of consistency and agreement between different studies, where the cost of a breach fluctuates depending on the estimator and the context. There are several reasons for this.

First, estimators are hamstrung by a lack of quality data. For most firms, attacks are rare and most attacks go unreported. Organisations have strong incentives not to report attacks as it reflects poorly on them. New mandatory reporting regulations will encourage firms to report more transparently, although these regulations usually do not extend to SMEs who will still have little incentive to report attacks and breaches. The reticence to report leads to many studies having small sample sizes which in turn hinders the accuracy of their findings. Further, most of these studies are conducted by private organisations, many of whom are also providers of

cyber security, which may impact their credibility. Notably, government studies tend to be much more conservative in their estimates than private sector studies.

The second reason for inconsistent risk measurement is there's a great deal of analytical confusion in the way measurement is executed. There is a large degree of variability which is often undescribed in these studies. The victim's identity, in terms of their organisation size and asset value, dictates the magnitude of their losses. The costs of an attack are also dependent on the nature of the attack and the types of assets which are compromised. Victims who surrender control of their website for a few hours suffer much less than victims who lose the personal details of millions of customers. The fact that losses can come from a variety of sources – such as financial setbacks in the form of detection, investigation, fines, and recovery services; or from less quantifiable damages to a firm's reputation – mean that each individual study on the cost of a cyber breach are conflating different slices of cyber criminal activity as the same phenomenon: a standard cyber 'breach'.

Estimates of the mean cost of a cyber breach

SOURCE: AlphaBeta analysis from various reports and studies: UK Dept for Digital (2018), Cyber Security Breaches Survey, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf; Juniper Research (2015), Cybercrime will cost businesses over $2 trillion by 2019, available at: https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion; Ponemon Institute and IBM (2016), Cost of Data Breach Study, available at: https://www-03.ibm.com/security/ca-en/data-breach/; Ponemon Institute and IBM (2017), Cost of Data Breach Study, available at: https://www.ibm.com/downloads/cas/ZYKLN2E3; Kapersky (2017), IT Security: cost-centre or strategic investment?, available at: https://go.kaspersky.com/IT-Security-Economics-Report.html; Ponemon and Accenture (2017), Cost of Cyber Crime Study, available at: https://www.accenture.com/au-en/insight-cost-of-cybercrime-2017; ACSC (2016), Cyber Security Survey, available at: https://www.cyber.gov.au/news/2016-australian-cyber-security-survey; Romanovsky (2016), Examining the costs and causes of cyber incidents, available at: https://academic.oup.com/cybersecurity/article/2/2/121/2525524.

3 THE CHALLENGE: AUSTRALIA NEEDS TO PLUG THE WORKFORCE GAP, REMOVE STARTUP BARRIERS, STRENGTHEN R&D, AND MEASURE GROWTH AND IMPACT

Protection measurements typically assess either readiness or spending on cyber

There are various existing methods and approaches to measure national and international levels of cyber security protection. Most of these are surveys seeking to estimate firm spending on cyber security and assess readiness to deal with threats. Much like studies on risk metrics, government studies on protection tend to be more robust than private sector estimates. For example, Statistics Canada and the United Kingdom's Department for Digital included measures of protection as well as risk in their previously mentioned studies, where they examined readiness of firms to deal with threats as well as quantifying spend on cyber security products and services. Several international organisations and private firms have also formulated readiness indices. Most of these indices aim to assess how prepared countries are to meet cyber threats (although there were two indices that assessed the readiness level of industries and firms by IBM and Accenture respectively).[63,64]

The other main area of protection that is sometimes measured is cyber security spending by organisations and at the country level. Again, this area presents data challenges because many organisations are understandably reluctant to disclose information on their cyber security expenditure given the value of that information to potential cyber attackers. Previously, the main source of information on cyber expenditure has been from market data providers such as Gartner and IDC, which sell international and national-level data on the values of sales in the cyber security or 'information security' market, both historically and as forward projections.[65,66] However, this data doesn't capture the full value of organisations' cyber security spending because it doesn't include wages paid to internal cyber security teams. More recently, government studies in Canada and UK have begun estimating overall spending on cyber security products, services and wages.[67,68]

Existing Australian measures of risk and protection have important limitations

Local measurements on risk and protection are undertaken by several government organisations: the Office of the Australian Information Commissioner (OAIC), ABS and ACSC within the Australian Signals Directorate. The OAIC releases a regular half-yearly national report on data breaches as part of its Notifiable Data Breaches Scheme, which monitors breaches of personal information across the nation as part of the federal Privacy Act. The ABS, as part of its annual survey on business use of IT (BUIT), enquires superficially about the cyber security incidences, readiness, and the impact of breaches. Finally, the ACSC is undertaking a survey of small to medium-sized businesses on the incidence of malicious cyber activity, their impact and the readiness of firms to deal with the consequences. The ACSC has also previously released a technical threat report which describes the proliferation of new methods and technologies being used by attackers as well as semi-regular surveys about readiness across both public and private sectors.

Thus, where government is required to have a clear role to play, relevant agencies do already measure most of the key metrics (Figure 48). However, the robustness of the metrics needs to be improved in order for the data to be informative and useful. This can be through using broader samples (as the ACSC has recently done), and also with better integration of different data sources across agencies. Government could also consider adding measurement of the cost of breaches in Australia.[69] Despite the methodological challenges associated with cost of breach studies, this information is important for organisations in evaluating their avoided losses from cyber investments and thus the impact of their cyber security investments. The work of Canadian and UK governments in this area has demonstrated that robust approaches are feasible.

63   IBM (2018) X-Force Threat Intelligence Index. Available at: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN.

64   Accenture (2017) Security Index. Available at: https://www.accenture.com/t00010101T000000Z__w__/au-en/_acnmedia/PDF-48/Accenture-The-Acn-Security-Index-new.pdf.

65   Gartner (2018) Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. Available at: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.

66   IDC (2019) Worldwide Semiannual Security Spending Guide. Available at: https://www.idc.com/getdoc.jsp?containerId=IDC_P33461.

67   Statistics Canada (2017) Cyber Security and Cybercrime in Canada. Available at: https://www150.statcan.gc.ca/n1/pub/71-607-x/71-607-x2018007-eng.htm

68   UK Department for Digital, Culture, Media & Sport (2018) Cyber Security Breaches Survey. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018.

69   Note that Australia's Cyber Security Strategy (2016) identifies an action to 'Sponsor research to better understand the cost of malicious cyber activity to the Australian economy', which the authors understand has not yet been delivered.

Figure 48

Cyber security in the broader economy – measuring risk

Measures of risk			Possible metrics (applicable at the level of the firm or economy)	Comments
Effective risk environment	Vulnerability	Pervasiveness of threats	• Incidence of attacks	
			• Proliferation of threats	
			• Accessibility of malicious tools (e.g. malware, spyware, worms, viruses)	
		Extent of digital risk exposure	• Proportion of **digital assets that are vulnerable**	• Too hard for government to accurately assess
			• Probability that these digital assets will be **compromised**	
			• **Criticality** of these digital assets	
	Impact of breach	Type of breach	• The type of impact in terms (e.g., data loss, loss of service)	
		Direct cost of cyber breach	• Financial cost of **detection**, **investigation** and **recovery** services, as well as **lost income** from interrupted operations and any **fines and penalties**	• May help organisations to make good investment decisions
		Indirect cost of cyber breach	• Financial **cost of lost future earnings** from losing current and prospective customers	
			• Opportunity cost of **slowing digitisation of operations slow** to mitigate cyber risk	

Figure 49

Cyber security in the broader economy – measuring protection

Measures of protection			Possible metrics (at the level of the organisation or economy)	Comments
Protection	Level of protection	Accessibility to protection	• Proportion of latest cyber protections available and affordable to firms	• Difficult for government to accurately assess as highly specific to different organisations
		Uptake of protection	• Types of threats protected against	
		Extent of digital assets secured by protections	• Proportion of digital assets that are protected	
		Readiness	• Readiness index describing a country's security capabilities, commitment, and maturity	• Can identify areas of national weakness for policy
	Cost of protection	Spend on cyber security products and services	• Value of investment in services and products from local sector	• Crucial for enabling organisations to benchmark their own investments
			• Value of investment in services and products imported from overseas	
		Spend on wages for in-house cyber professionals	• Value of wages on internal cyber teams	

3 THE CHALLENGE: AUSTRALIA NEEDS TO PLUG THE WORKFORCE GAP, REMOVE STARTUP BARRIERS, STRENGTHEN R&D, AND MEASURE GROWTH AND IMPACT

In protection, there are more substantial gaps in the metrics that could be filled by government (Figure 50). The level of protection is touched on in the ABS' survey on business uses of IT (BUIT), but not in great depth. The need for government to support measurement is especially urgent when it comes to assessing cyber readiness throughout the economy and in estimating the cost of protection. Assessing cyber readiness across industries and geographies can reveal gaps in Australia's cyber defences whilst cost of protection studies provides benchmarks to which firms can compare their own levels of protection.

The economic benefits of cyber security have been analysed the least to date

Despite the obvious value of a stronger understanding of the benefits of cyber security in the economy, there is very little existing work to objectively measure or assess these benefits – either internationally or in Australia. This is likely a reflection of both the relative novelty of cyber security, but perhaps more significantly the methodological challenges of understanding and measuring benefits. Unlike some other types of investment, cyber security often does not generate a direct return and enables value creation in other ways.

There are two main ways through which cyber security benefits manifest. First, cyber security protects firms against losses from cyber security attacks. This is most applicable at the organisational level, where avoided attacks translate to avoided costs relating to dealing with and recovering from an attack. Second, cyber security protects and enables sources of economic value. There are a range of digital industries and activities, such as e-commerce, online banking and cloud computing, which have become prominent and indispensable features of the Australian economy. These activities are utterly contingent upon cyber security's protection. That is, it would be impossible to conduct many important digital enterprises in cyber space that is not secure.

Cyber benefits have not been well studied to date. There are no Australian Government studies into these two aspects of cyber security benefits, and few private sector analyses. One of the few private sector reports which touched on benefits was by the consultancy BDO as part of a broader survey on cyber risk. BDO compared the incidence of attacks on surveyed firms with and without cyber security protocols which improved their risk visibility, finding that protected firms were less likely to experience malicious attacks.[70] This was a peripheral component of the report and although the survey covered nearly five hundred respondents, the sample of surveyed firms was not representative of the economy at large.

Two other measurements have focused on the enabled or protected value, including one analysis in Australia. Deloitte, a consulting firm, used CGE economic modelling to estimate the impact of firm investment in cyber security products and services on GDP, business investment, wages, employment, national revenue, and the terms of trade.[71] The results claimed a 5.5 per cent lift in overall business investment across the economy as a result of cyber security products and services bought, however the underlying analytical assumptions are not clear. In 2015, the Atlantic Council in conjunction with Zurich Insurance Group released long-term modelling of the economic benefits and costs of various scenarios for global cyber security to 2030.[72] While this analysis provides a powerful case for the economic benefits of cyber, it does not consider the implications of alternative cyber scenarios in different countries.

70 BDO Australia (2018) 2017/2018 Cyber Security Survey. Available at: https://www.bdo.com.au/en-au/20172018-cybersecurity-survey-results

71 Deloitte Australia (2017) What's over the horizon? Recognising opportunity in uncertainty.
    Available at: https://www2.deloitte.com/au/en/pages/building-lucky-country/articles/whats-over-horizon.html.

72 The Atlantic Council and Zurich Insurance Group (2015) Overcome by cyber risks? Economic benefits and costs of alternate cyber futures.
    Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/risk-nexus-overcome-by-cyber-risks-economic-benefits-and-costs-of-alternate-cyber-futures/.

Cyber security benefits the economy through a range of different pathways

Cyber security protects and generates value for the economy through a range of different pathways and part of the measurement challenge is in understanding these pathways in more depth. For example, cyber protection supports digitisation. Confidence in their cyber security protection encourages firms to digitise their operations as well as collaborate digitally, thereby improving information exchange in the economy leading to improved productivity and creating the opportunities for innovation. Five example pathways are outlined in Figure 50 below, although there are undoubtedly other pathways that could be proposed. Each is worthy of further study.

A more unified approach to measuring the benefits of cyber security would be through estimating changes to economic value captured as a result of digital innovation. Such a measurement

approach would directly demonstrate how investments in cyber security support economic growth. This could be done by developing counterfactual scenarios that model different levels of cyber security investment and estimate the resultant differences in economic value or output, at the level of the Australian economy. The approximate difference between the counterfactual scenarios roughly equates to the value protected by cyber investments.

Proposals to further develop measurement of cyber security risks, protection, and benefits are described in Chapter 4, including strengthening existing government measurements and trialling new approaches to analysing the impact of cyber security on the economy.

Figure 50

Pathways for economic value of cyber security
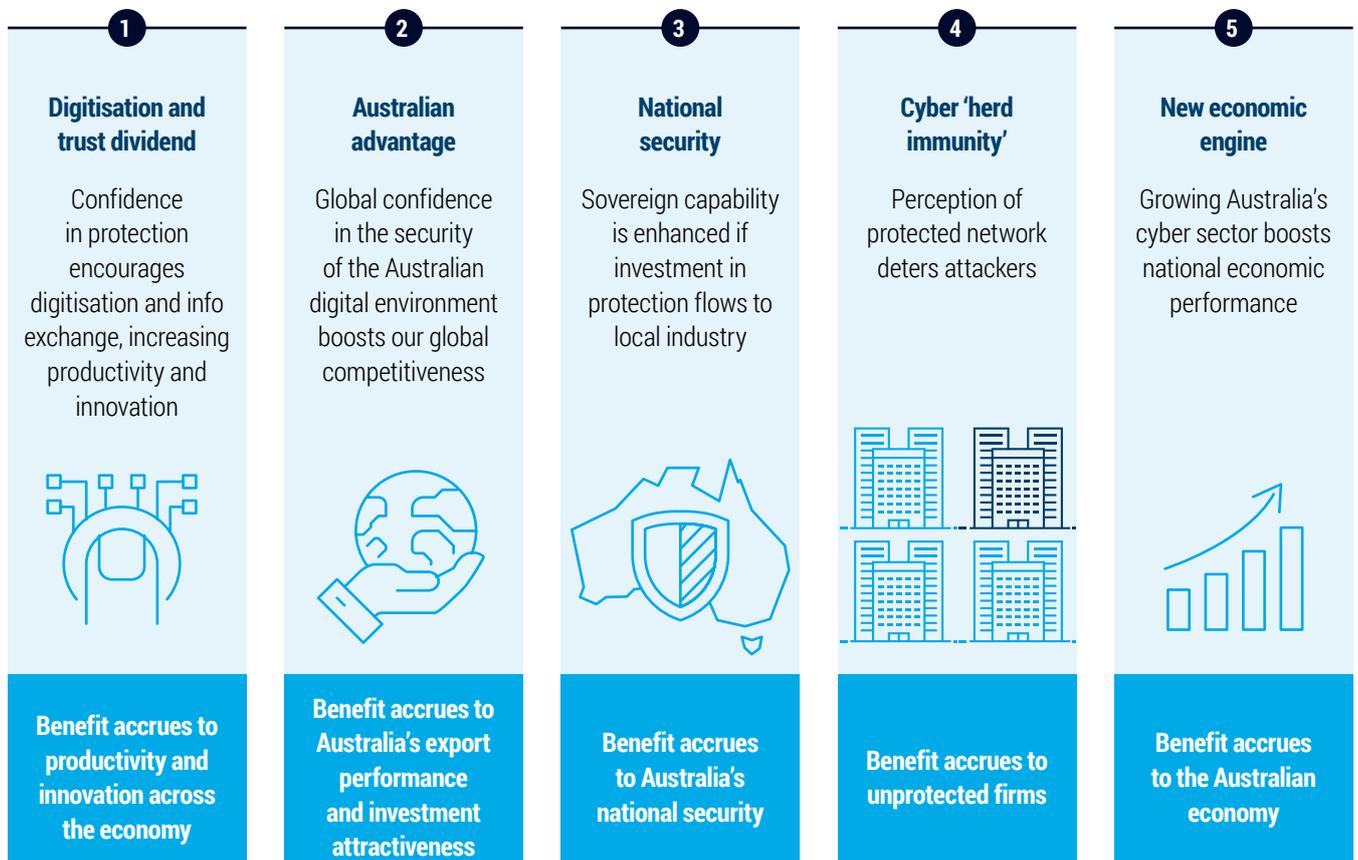
1	2	3	4	5
Digitisation and trust dividend	**Australian advantage**	**National security**	**Cyber 'herd immunity'**	**New economic engine**
Confidence in protection encourages digitisation and info exchange, increasing productivity and innovation	Global confidence in the security of the Australian digital environment boosts our global competitiveness	Sovereign capability is enhanced if investment in protection flows to local industry	Perception of protected network deters attackers	Growing Australia's cyber sector boosts national economic performance
Benefit accrues to productivity and innovation across the economy	**Benefit accrues to Australia's export performance and investment attractiveness**	**Benefit accrues to Australia's national security**	**Benefit accrues to unprotected firms**	**Benefit accrues to the Australian economy**

4 BUILDING A COMPETITIVE AUSTRALIAN CYBER SECURITY SECTOR

Key points in this chapter

- **Much has been achieved** since the Sector Competitiveness Plan was first published in 2017

- But **more action is needed** to grow vibrant and competitive cyber security sector, that generates increased investment and jobs for the Australian economy

- Urgently need to address **skills and workforce shortage**

- **Greater awareness** to attract best and brightest to sector

- **More pathways** for workers to transition from broader IT sector and other industries

- **Better collaboration** in R&D

- **Concentrate R&D** on areas of strength and sector segments of software, security operations, and underlying processes

- **Support local companies** to grow, mature and export solutions

> "
> Much has already been achieved... but more needs to be done to fully seize the tremendous opportunity in cyber security

This Sector Competitiveness Plan shows great potential for Australia to become a leading global exporter of cyber security software and services where it already has a competitive advantage (see focus segments in Chapter 2).

However, Australia cannot expect to build on its existing strengths and develop a vibrant cyber security sector without properly addressing existing challenges, such as:

- creating a sharper focus in the funding of cyber security research;

- removing growth hurdles for small local cyber startups; and

- increasing the pool of job-ready cyber security workers in the short- and long-term.

Given the urgency of this opportunity and the eagerness of many other countries to also seize the moment in cyber security, action needs to happen fast.

Much has been achieved already since the initial Sector Competitiveness Plan was first published in 2017. Recognising the strategic growth potential of cyber security, the Australian Government has established a new Cyber Security CRC, which will provide more targeted funding for the country's most promising research projects. The Government also launched AustCyber's GovPitch, a new initiative to help cyber security startups in Australia win public sector contracts more easily.

The education system has also responded well to the challenge with half of the universities in the country now offering a specific cyber security degree or IT degree with a major in cyber security.

AustCyber has committed to a regulatory reform plan that focuses on regulation and standardisation of cyber security (see Appendix C).

Much has already been achieved... but more needs to be done to fully seize the tremendous opportunity in cyber security.

Still more needs to be done to enable Australia to fully seize the tremendous opportunity in cyber security. To develop a highly capable and globally competitive cyber security sector, Australia should pursue three goals, as illustrated in Figure 51:

- develop a competitive cyber security ecosystem;

- strengthen the exportability of local cyber security companies; and

- capitalise on Australia's quality education system to become a leader in cyber education.

4 BUILDING A COMPETITIVE AUSTRALIAN CYBER SECURITY SECTOR

An overview of the key elements of the Sector Competitiveness Plan

Key goals

1 Grow an Australian cyber security ecosystem

2 Export Australia's cyber security to the world

3 Make Australia the leading centre for cyber education

Strategies

Grow an Australian cyber security ecosystem
- Help cyber security startups find their first customers
- Improve research focus and collaboration to assist commercialisation
- Make access to seed and early-stage venture capital easier
- Simplify government and private sector procurement processes
- Provide robust measurement of the ecosystem's development and impact on the Australian economy

Export Australia's cyber security to the world
- Support Australian firms to develop scalable service delivery models
- Develop cyber security as an educational export
- Attract multinational corporations to use Australia as an export base for the region

Make Australia the leading centre for cyber education
- Attract and retain the best and brightest to cyber security
- Create vibrant, industry-led professional development pathways
- Ramp up cyber security education and training

Potential outcomes by 2026*

- Revenue of Australia's cyber software segment increased by **$600m**
- **80%** of cyber research funding spent in focus areas

- Australia becomes the leading regional base for cyber security
- Australia's cyber services export revenue grown by **5x**
- Revenue from international education services in cyber increased by **10x**

- At least **double** the number of cyber security professionals in Australia
- Dynamic, technical and non-technical career path-ways in cyber that are visible to the labour market

* These are only initial estimates for potential outcomes and would need to be refined by AustCyber through further analysis

4.1 GROWING AN AUSTRALIAN CYBER SECURITY ECOSYSTEM

To become a global market leader in cyber security and serve a substantial share of additional security demand over the next decade, Australia is building a stronger, more coherent cyber security ecosystem. Australia's cyber security sector lacks the strong domestic ecosystem to compete effectively on a global scale. The local network of specialist companies, researchers, government bodies and training institutions that make up Australia's cyber security sector remains fragmented and underdeveloped, especially in software. This makes it difficult for Australia to fully harness the tremendous economic opportunity arising from the expected surge in demand for cyber security.

To become a global market leader in cyber security and serve a substantial share of additional security demand over the next decade, Australia is building a stronger, more coherent cyber security ecosystem.

To achieve this, Australia needs to create more innovative cyber security startups and help them grow into mature, market-ready and internationally competitive businesses that can cater for the domestic market as well as global value chains. Strengthening the cyber security ecosystem also means inspiring greater collaboration between companies, researchers, government, investors, education providers, and other stakeholders involved.

Help cyber startups find their first customers

Anchor customers, typically large industry players or government departments, add value to any startup. But for cyber security startups, which rely heavily on trust to gain access to high-risk business areas, anchor customers are one of the most critical ingredients for success as they help establish market legitimacy.

Assisting cyber security startups in their search for customers can help strengthen the competitiveness of the local industry. This is because anchor customers often challenge an emerging company to sharpen its profile and refine its offering to be better aligned with global market needs, which increases business prospects.

🔍 **Explore**

↗ **Action**

Actions to help startups

Action	Lead actor	Status
Improve access to first customers for Australian startups by: • Analysing the barriers and risks for government agencies and established businesses working with startups • Promoting strategies to mitigate these, for example, piloting, investment partnerships • Providing access to business coaching for startups • Showcasing Australian cyber security products and services to potential customers.	AustCyber	↗
Recommendation that the Australian Government encourage industry investors in the CSIRO Innovation Fund to also become first customers for Australian cyber security startups the Fund supports.	Government and industry	🔍
Startups and small organisations mature business operations and systems to work effectively with first customers.	Industry	↗

4 BUILDING A COMPETITIVE AUSTRALIAN CYBER SECURITY SECTOR

Improve research focus and collaboration to assist commercialisation

Australia is home to several world-class universities and research institutions on the leading-edge of cyber security innovation. However, a diffuse funding system and weak links between academics and business limit the effectiveness of Australia's research capabilities.

Australia needs to replace this scattered approach to public R&D funding for cyber security with a more targeted funding strategy that focuses on cultivating a select number of national hubs for research excellence. A limited and specific set of research areas would also help focus the efforts of Australia cyber security researchers and institutions, and guide the allocation of funding to research by government agencies.

AustCyber has developed Knowledge Priorities for cyber security in consultation with industry and researchers (see Appendix A). The knowledge priorities will guide industry research needs and commercialisation opportunities for Australia's cyber security sector, as well as to inform AustCyber's activities as it works with stakeholders across the economy to improve the sector's research focus, collaboration and commercialisation outcomes. These knowledge priorities will be refined over time through further engagement and an evaluation of areas of existing research capability in Australia.

Further, Australia should work to improve opportunities for research collaborations between industry and universities. A stronger innovation partnership is needed to fully harness the commercial possibilities of cutting-edge research.

Explore

Action

Actions to improve research and commercialisation

Action	Lead actor	Status
Identify areas of research strength that support the initial focus segments, based on Australia's existing research capabilities.	AustCyber	Action
Work with government/s to better support short and longer-term cyber security research that will ensure both commercialised outcomes and development of scaled national research capability.	AustCyber, with government agencies	Explore
Work with Data61 to develop research translation and product management models that can be implemented in cyber security research institutions.	Research institutions	Action
Establish a directory of Australian academics created to help businesses connect with research expertise, including cyber security.	Data61	Explore
Invest in the development of stronger collaboration capabilities, including offering work placements for postgraduate students.	Industry	Action
AustCyber to work closely with the Cyber Security CRC to assist in developing industry-university collaborative proposals and promoting resulting commercialised products.	AustCyber/CRC collaboration	Action

Make access to seed and early-stage venture capital easier

Australian cyber security companies face larger obstacles than some of their global peers when trying to access early-stage venture and seed capital.

It is crucial for Australia to remove these funding hurdles and help startups commercialise novel products and innovative services that will differentiate them from foreign rivals. A more favourable funding environment, including the system of incubators and accelerators, will enable Australian cyber security startups to become global market leaders.

> Australian cyber security companies face larger obstacles than some global peers when trying to access early-stage venture and seed capital

🔍 **Explore**

↗ **Action**

Actions to improve access to early-stage capital

Action	Lead actor	Status
Increase the availability of and access to early-stage funding for startups by: • ensuring startups have adequate information about the range of potential funding sources • identifying and attracting additional funding sources, for example international venture capital funds entering Australian market, better access to investments made by Australian superannuation and wealth funds.	AustCyber	↗
Form an informal panel of CIOs and CISOs that can rapidly vet startups' products for venture capital investment.	AustCyber	🔍
Develop the scale and maturity of incubators and accelerators that have a cyber expertise.	AustCyber	↗

4 BUILDING A COMPETITIVE AUSTRALIAN CYBER SECURITY SECTOR

Simplify government and private sector procurement processes

Many large companies and government agencies – both state and national level – are bound by strict procurement guidelines, designed to ensure reliable performance of contractors and protect the integrity of their networks. But the complexity and cost of these requirements pose a barrier for smaller and newly established companies, which are often defeated by larger rivals with more experience, reputation and resources.

The complexity and cost of procurement requirements pose a barrier for smaller and newly established companies

While strict compliance and procurement rules are necessary to protect high-risk business areas, more can be done to ensure a greater participation of startups and other small companies in providing cyber security products and services to government and big corporates.

🔍 **Explore**

⬈ **Action**

Actions to simplify procurement

Action	Lead actor	Status
Support greater access to government and larger business procurement opportunities by: • analysing the contract size and structure of existing cyber security contracts and recommend actions, for example introducing maximum contract sizes • Working with state and Australian Government agencies to identify opportunities for piloting of technologies offered by Australian companies.	AustCyber	🔍
Recommendation that the Australian Government partially subsidise the costs of Australian Government product certification (for example, Evaluated Products List (EPL)) and service accreditation (for example, Information Security Registered Assessors Program (IRAP)) for Australian small to medium enterprises.	Government	🔍
Innovate around procurement processes to identify requirements that can be relaxed for startups and SMEs.	Industry	⬈
Work in partnerships with key stakeholders – governments, regulators, industry – to explore opportunities for harmonising local standards and regulations with international standards.	AustCyber	⬈
Advocate on behalf of industry in discussions on the particular issues that may attract regulatory responses, exploring the impact of such actions.	AustCyber	⬈
Work with Australian Government agencies supporting regular industry consultation to facilitate innovation and export opportunities within the regulatory framework.	AustCyber	⬈
Work with industry associations and other peak bodies to ensure industry interests are represented in boosting the availability of skilled cyber workers including temporary visas.	AustCyber	⬈

Provide robust measurement of the sector's development and impact on the Australian economy

A healthy, mature cyber security sector has strong growth prospects, long lines of interested investors, innovative sector development policies and a deep talent pool. Fundamental to accomplishing this vision is a robust common fact base of the sector and its impacts. Such a fact base requires measurements of the sector to improve. Developing high-quality measurement projects will require close collaboration between industry and government in order to draw together funding, expertise and credible data.

Studying the impacts of cyber security further fills an important knowledge gap. Developing more robust measures of risk, protection and benefits is not simply of scholarly interest but such knowledge has commercial and national security implications. Whilst concepts of risk and protection are well understood in cyber security, the current state of knowledge can be improved with more committed investment on behalf of government to produce a broader suite of measures. The benefits of cyber security are very poorly understood and significant progress can be achieved by implementing relatively straightforward and practical actions.

🔍 **Explore**

↗️ **Action**

Actions to improve measurement of cyber security

Action	Lead actor	Status
Develop and implement a robust and repeatable interim sector measurement	AustCyber, with government agencies across levels and industry	↗️
Recommendation that the Australian Government institute a regular and comprehensive measurement of the sector.	Government	🔍
Recommendation that the Australian Government gather better quality information on the levels of risk faced by different organisations, and the current state of protection from cyber threats.	Government	↗️
Undertake analysis of the overall economic value of capital investments in cyber security companies; and organisational investment in cyber capabilities.	AustCyber	↗️
Improve understanding of the pathways through which cyber generates economic value.	AustCyber and industry	↗️

4.2 EXPORTING AUSTRALIA'S CYBER SECURITY TO THE WORLD

Mounting cyber threats will drive future demand for effective security solutions across Australia and unlock new business opportunities for security providers. Yet the limited size of the local market demands that cyber security companies develop and maintain a strong export focus. For Australia to become a leading cyber security provider in the Indo-Pacific region, local companies will need to improve export capabilities. Australia should also investigate ways to become a more attractive base for cyber security exports of multinational corporations.

Many local cyber security companies still lack the scale to effectively compete in markets outside Australia but this is changing

This is particularly evident for cyber security services companies, which appear to face greater difficulties than hardware and software providers to venture abroad and establish an international market presence. In light of existing country-specific strengths (trade data indicates Australia is already 'punching above its weight' and earns a relatively higher revenue with services than its peers), boosting the export capabilities of local cyber security services companies would deliver particularly strong economic gains.

Support Australian companies to develop more scalable business models

The key obstacle for many Australian cyber security companies, especially in services, is a lack of scalability in their business models. This means they cannot easily grow in order to capture opportunities, and export relies on expanding their workforce offshore in ways that are often too difficult. Working with Australian cyber security companies to improve the scalability of their businesses will be critical to export growth.

🔍 **Explore**

↗ **Action**

Actions to increase exports

Action	Lead actor	Status
Work with government/s to deepen the understanding of export opportunities for Australian cyber security through a detailed market analysis.	AustCyber, with government agencies	🔍
Analyse the amenability of Australia's existing services strengths to remote delivery models (particularly in the protection stack).	AustCyber	↗
Work with government/s to map possible target markets for Australian-managed services in the protection stack and the specific barriers to export to those countries.	AustCyber, with government agencies	🔍
Identify ways to increase scale through partnerships and invest in the development of scalable, managed service models.	Industry	🔍

Develop cyber security as an educational export

In recent years, education has become one of Australia's largest export earners, rivalling the country's top resources exports.[1] This trade success is a testament to Australia's strong reputation and infrastructure in international education and training, and signals a powerful opportunity for cyber security service providers.

Australia has the potential to become the leading regional, if not global, provider of cyber security education and training. However, realising this potential requires a new focus on growing our cyber security education and training institutions into dynamic, enterprising and export-oriented players.

> "
> Realising Australia's potential in cyber education requires new focus on growth and national coordination

Explore

Action

Actions to develop cyber security education exports

Action	Lead actor	Status
Establish marketing presence in cyber security in key target markets and develop partnerships with local industry that have training needs.	Education and training institutions	🔍
Recommendation that the Australian Government, working with AustCyber, support training institutions to export cyber security by: • identifying target markets for cyber security education exports • Promoting cyber security as a national strength within existing Australian education exports campaigns (for example, Future Unlimited).	Government, with AustCyber	🔍

---

1   Australian Government, Department of Foreign Affairs and Trade (2017), *Composition of Trade Australia 2015–16*. Available at: http://dfat.gov.au/about-us/publications/Documents/cot-fy-2015-16.pdf.

Attract multinational corporations to use Australia as an export base for the region

Large multinational corporations currently meet most of Australia's cyber security needs. They play an important role, not just as security providers, but also as employers. However, interviews indicate that foreign cyber security providers use their Australian operations almost exclusively to service the local market.

Australia could capitalise further on the presence of multinational corporations by encouraging them to make better use of the proximity to Asia and Australia's potential to serve as a regional export base. Many foreign companies are already attracted to Australia because of the stable political environment, favourable business climate, and diverse and well-educated workforce.

A range of incentives could encourage multinational cyber security companies to broaden their local operations and ship a larger share of exports from Australia. Multinationals could significantly boost Australia's export capabilities in cyber security, particularly in services, where local companies are generally most challenged to rapidly improve their export-readiness. Multinational companies, in contrast, already have the necessary scalability that allows them to more easily expand into global markets.

> Australia could capitalise further on the presence of multinational corporations

🔍 **Explore**

↗ **Action**

Actions to attract multinationals to use Australia as export base

Action	Lead actor	Status
Conduct detailed analysis of the existing export benefits of Australian operations of multinational corporations, and identify areas of comparative advantage for Australia as a cyber security export base for multinational corporations.	AustCyber	↗

4.3 MAKING AUSTRALIA THE LEADING CENTRE FOR CYBER SECURITY EDUCATION

Cyber security companies worldwide are struggling to expand their businesses, as they cannot find enough skilled workers to satisfy the burgeoning demand for security products and services. There are signs, however, that the talent drought affecting cyber security companies in Australia is among the most acute globally. The number of job-ready candidates that Australia's education system produces is inadequate to meet current industry demand. While universities and TAFEs have begun to launch new study courses, they will not generate the graduate volume needed in the short to medium-term to keep pace with the sector's rapid expansion.

This skills shortage needs to be addressed quickly. It is already hindering the growth of the Australian cyber security sector. This problem will only magnify in the future as more cyber security providers edge into the market, drawn by the prospect of servicing the growing global security demand. Without a strong education and training system that provides cyber security companies with a robust pipeline of employable graduates, Australia will struggle to grow its cyber security ecosystem and become a leading exporter of cyber security. This makes resolving the skills challenge an economic imperative – it lays the groundwork for any other strategy to advance the competitiveness of Australia's cyber security sector.

Resolving the skills shortage is an economic imperative

The responsibility doesn't lie solely with universities and other higher-education providers, but also with vocational training organisations and industry itself. Australian companies need to offer more, and better, opportunities for 'on-the-job' training of cyber security graduates. Meanwhile, more programs are needed to help equip professionals from various backgrounds with cyber security relevant skills, so they can transition into the industry.

The establishment of the TAFE cyber Reference Group early in 2018, and plans to setup a similar university cyber training reference group – both coordinated by AustCyber – will be important to ensure the effective ownership for many of the actions identified below.

Attract the best and brightest to cyber security

Because cyber security is a nascent industry, many education providers have only recently begun to include relevant courses in their curricula. While universities and vocational training organisations increasingly promote cyber security as an attractive career path, many students are not yet fully aware of the strong job opportunities for cyber security professionals.

In addition to promoting science, technology, engineering and mathematics (STEM), high schools could play a bigger role in nurturing an early interest in cyber security and preparing students for a career in this dynamic, fast-growing industry. There is also an opportunity for employers to sponsor scholarships with work-integrated learning to attract high-quality students and improve the job-readiness of graduates.

🔍 **Explore**

↗ **Action**

Actions to attract more students

Action	Lead actor	Status
Recommendation that the AustCyber and other relevant stakeholders work with government/s to expand awareness of cyber security careers in high schools by: • improving the available information on career paths and role definitions in cyber security • scaling existing efforts to promote cyber security as a career for women • expanding cyber challenges programs in schools to increase the awareness and attractiveness of cyber career paths.	AustCyber, government and other relevant stakeholders	↗
Increase the number of *employer-sponsored scholarships that incorporate work-integrated learning opportunities* for high-school students and consider 'return of service' obligations to encourage students to remain in Australia.	Employers and training institutions	↗
Introduce a voluntary 'Digital Nation' program, where post-secondary students gain work experience in digital professions including cyber security.	AustCyber, with employers	🔍

Note: actions that have been added or updated since the release of the first Sector Competitiveness Plan in 2017 are in *italics*.

4 BUILDING A COMPETITIVE AUSTRALIAN CYBER SECURITY SECTOR

Ramp up cyber security education and training

Cyber security education and training is ramping up among universities and TAFEs. Two TAFE cyber security non-degree courses are being rolled out at a number of TAFEs around the country, and nearly half of all universities now offer either a specific degree in cyber security or an IT or computer science degree with cyber security as a major.

However, it is critical that the student demand for course places also grows and that cyber education remains financially sustainable. It is also important to maintain high quality education provision during a period of rapid expansion, to ensure that graduates are job-ready.

Employers and training institutions should continue to look for ways to work together to tackle the skills shortage and provide more opportunities for targeted cyber security training. Several high-profile partnerships between industry and training institutions, for example between Optus and Macquarie University or between Commonwealth Bank of Australia and the University of New South Wales, have emerged in recent years. They can serve as a blueprint for further collaborations to increase Australia's pool of cyber security workers with industry-relevant skills.

🔍 **Explore**

↗ **Action**

Actions to increase cyber education and training

Action	Lead actor	Status
Increase the supply of cyber education teaching by: • developing practical ways to attract and retain teachers, including by offering financial incentives and more flexible position structures (for example, teaching-only roles in universities, part-time roles in TAFEs) • developing a national approach for expanding the pool of guest lecturers, including leveraging guest lecturers through other channels.	AustCyber and training institutions Employers and training constitutions	🔍 ↗
Recommendation that governments mitigate upfront costs of setting up courses by: • including cyber courses on all states and territories skills' lists and lifting government courses subsidies for cyber vocational education and training courses to better fund upfront infrastructure development costs • increasing direct financial support to universities and TAFEs to set up world-class cyber security infrastructure to support skills development.	Government	🔍

Action	Lead actor	Status
Adopt a national skills framework based on the NICE Cybersecurity Workforce Framework to help build a common understanding between industry and education about skills needs and curriculum relevance, and map course curricula to this framework.	AustCyber, employers and training institutions	↗
Recommendation that the Australian Government extend and expand the Academic Centres of Cyber Security Excellence program, including a practical, challenge-based assessment framework, and develop a companion Training Centres program.	Government	🔍
Release comprehensive cyber security-specific performance metrics, for example graduate numbers, performance in cyber security challenges, employment outcomes and teaching quality metrics.	Training institutions	↗
Increase the attractiveness and relevance of cyber security programs at Australia's universities and vocational training institutions by working closely with employers in: • seeking opportunities to build *work-integrated learning* into curricula • regularly revising curricula and course structure to maintain relevance.	Training institutions	↗
Ensure senior executives, board directors and policymakers have access to high-quality cyber security training programs.	AustCyber	↗

Note: actions that have been added or updated since the release of the first Sector Competitiveness Plan in 2017 are in *italics*.

4 BUILDING A COMPETITIVE AUSTRALIAN CYBER SECURITY SECTOR

Create vibrant, industry-led professional development pathways

The talent shortage in cyber security is exacerbated by employers' concern that graduates from university programs are not job-ready. Opportunities to transition workers from other adjacent parts of the IT sector and the broader workforce are also being missed.

Offering visible and attractive pathways for the professional development of cyber security workers would be an important step towards addressing both these issues. This means creating clearer training options for general IT workers who are interested in transition to cyber security roles, and improving opportunities for on-the-job training, including graduate programs, which are currently limited to larger Australian companies.

🔍 **Explore**

↗ **Action**

Actions to create professional development pathways

Action	Lead actor	Status
Undertake market research to understand the specific barriers to transition that potential cyber workers report.	AustCyber	↗
Expand the range of training/re-training and transition models available by: • increasing the number of training places in lower cost course, such as vocational education and training short courses, micro-credentials and graduate certifications • establishing an apprenticeship model for cyber security that will enable more hiring of graduates, *with potential funding through the Skilling Australians Fund*.	Training institutions and employers	↗
Recommendation that the Australian Government consider increasing the relative affordability of training through subsidised training places for workers from disadvantaged backgrounds and fee waivers for specific cohorts of students.	Government	🔍
Improve the on-the-job training opportunities and clarity of career progression options to increase retention and link this to common messaging on the importance of cyber security to Australia's national interests.	Industry	🔍
Develop and propagate a rapid transition model for large- and mid-sized employers that helps them identify target workers and match them to appropriate training opportunities.	AustCyber	↗

Note: actions that have been added or updated since the release of the first Sector Competitiveness Plan in 2017 are in *italics*.

SUMMARY OF PROGRESS AGAINST ACTIONS

The scorecard below summarises progress against actions identified in the release of the first Sector Competitiveness Plan in 2017. Progress descriptions are not exhaustive, but rather capture the range of activity occurring across government, industry, training institutions and the research community, as well as within AustCyber itself. These activities are all aimed towards the improvement of the competitiveness of Australia's cyber security sector.

As this update to the Sector Competitiveness Plan is released, a focus on national level activity for AustCyber and the sector is contributing to the development of Australia's 2020 Cyber Security Strategy. The new strategy will be the successor to *Australia's Cyber Security Strategy*, released in 2016, which led to the establishment of AustCyber and a range of other measures to support the development of the sector. The Australian Government released a discussion paper calling for views on the strategy. AustCyber's response is available here.

A. Grow an Australian cyber security ecosystem

Target of initiative	Actions listed in 2017	Lead	Actions to-date (non-exhaustive)	Status
Help cyber startups to find their first customers	Analyse barriers and risks for government agencies and businesses to working with startups and promote strategies to mitigate these barriers (for example, via piloting and investment partnerships)	AustCyber	• AustCyber has had ongoing discussions with Commonwealth and state/territory agencies and larger businesses on barriers, with particular focus on procurement • AustCyber's National Network of Cyber Security Innovation Nodes are partnerships with state/territory governments to develop local capabilities and tackle local barriers, especially those relating to procurement and innovation practices	In progress
	Provide access to business coaching for startups	AustCyber, with relevant government agencies	• AustCyber has held several rounds of GovPitch, a forum where startups can pitch technical solutions to public sector executives, making it easier for them to apply for government cyber security contracts. The next round of GovPitch will take place in the first quarter of 2020 • AustCyber and Austrade coach and advise firms on business models, opportunities and strategic planning in order to establish themselves in overseas markets such as ASEAN, the US and the UK • Cyber security is now listed as a sector that can access business coaching services through Business.gov.au	Ongoing

4 BUILDING A COMPETITIVE AUSTRALIAN CYBER SECURITY SECTOR

A. Grow an Australian cyber security ecosystem

Target of initiative	Actions listed in 2017	Lead	Actions to-date (non-exhaustive)	Status
Help cyber startups to find their first customers	Promote Australian cyber security products and services to potential customers	AustCyber with Austrade, DFAT and the Australian British Chamber of Commerce	• Trade and investment delegations have showcased Australia's cyber security products and services to potential customers in various countries, including the US, UK, Germany, New Zealand, Singapore, India, Israel and Indonesia	Ongoing
	Recommend that the Australian Government encourages industry investors in CSIRO Innovation Fund to become first customers of cyber security startups that the fund supports	AustCyber (Advocacy) Government Industry	• Delivered as part of Main Sequence's work, which AustCyber is engaged with	Not continued
	Help startups, micro companies and small organisations to mature their business operations and systems	Industry	• AustCyber's Project Funds initiative assists with commercialisation, scaling and research activities • AustCyber refers startups to relevant state and territory small business programs through its National Network of Cyber Security Innovation Nodes	In progress

Target of initiative	Actions listed in 2017	Lead	Actions to-date (non-exhaustive)	Status
Improve research focus and collaboration to assist commercialisation	Identify areas of research strength that support the initial focus segments based on existing research capabilities	AustCyber and the Cyber Security Research Centre (Cyber Security CRC)	• AustCyber has been successful in ensuring the Australian Government's CRC Programme, Linkage Grants Programme and the research activities of Data61 have stronger ties to the Knowledge Priorities in this plan	In progress
	AustCyber to work with governments to support short- and long-term cyber security research that has the potential to lead to commercialised outcomes and scaling of national research capability	AustCyber, with government agencies	• Cyber Security CRC has been established and is working with more than 20 partners across industry, research and government sectors to support scaling and commercialisation of Australian cyber security research • AustCyber's Projects Fund is investing $15 million over three years to advance national priorities, including research and commercial capabilities	In progress
	Work with Data61 to develop research translation and product management models to be implemented in research institutions	Research institutions	• AustCyber participates in Data61's *D61+Live* events, which are thought leadership forums aimed at driving collaboration across technology sectors	In progress
	Establish a network of researchers and organisational practitioners to better connect researchers with industry future needs and identify challenges and opportunities	Data61 (previously assigned to AustCyber)	• Expert Connect, developed by Data61, was launched in 2017. It is a directory of Australian academics created to help businesses connect with research expertise, including cyber security	Completed
	Invest in the development of stronger collaboration capabilities including work placements for postgraduate students	Industry	• AustCyber supports Data61's online skills matching platform Ribit, which brings together tertiary graduates with STEM and digital skills employers, by partnering to deliver a cyber security specific stream in the platform	Ongoing

4 BUILDING A COMPETITIVE AUSTRALIAN CYBER SECURITY SECTOR

A. Grow an Australian cyber security ecosystem

Target of initiative	Actions listed in 2017	Lead	Actions to-date (non-exhaustive)	Status
Make access to seed and early-stage investment capital	Ensure startups have adequate information about available funding	AustCyber	• AustCyber provides companies with informal advice about potential funding sources • AustCyber is also deepening engagement with investors to further fuel ecosystem growth	In progress
	Identify and attract additional funding sources, such as venture capital	AustCyber	• AustCyber has ongoing engagements with several international capital groups aligned with national interests • AustCyber and the Australian Investment Council have partnered to increase knowledge of funding for investors into Australian deep technology and cyber security • AustCyber supports Austrade's promotion of opportunities to international investors	In progress
	Form informal panel of CIOs and CISOs to rapidly vet startup products for venture capital investment	AustCyber	• AustCyber and CISO Lens have collaborated to identify and assess startup products and commercialisation opportunities. CISO Lens also assists AustCyber in evaluating investment opportunities	In progress
	Develop the scale and maturity of incubators and accelerators with cyber security focus	AustCyber	• AustCyber is working on improving the effectiveness of existing accelerators and incubators related to cyber security • AustCyber works with CyRise, Australia's only cyber security accelerator to advance their bootcamps. CyRise is funded by the Victorian Government in partnership with Deakin University and NTT	In progress

Target of initiative	Actions listed in 2017	Lead	Actions to-date (non-exhaustive)	Status
Simplify government and private sector procurement processes	Greater access to procurement by governments and large businesses by analysing contract size, structure and regulations	AustCyber	• (Refer to previous page, plus:) • AustCyber assists DFAT to carry out their Cyber Capability Engagement Program (CCEP) which aims to build cyber security capacity across the Indo-Pacific. Three Australian firms have been procured to begin this project • AustCyber has recommended to the Federal Government that, as part of its new National Cyber Security Strategy, at least one per cent of government procurement be from the local ecosystem, growing to five per cent in the future	In progress
	Work with Australian and state/territory government agencies to identify opportunities for piloting technology	AustCyber	• AustCyber has held several rounds of GovPitch, an initiative which helps Australian cyber security startups pitch technical solutions to government officials, improving their chances of winning a government contract. The next round of GovPitch will be held in the first quarter of 2020 • AustCyber has assisted states and territories to take a greater interest in drawing on local capabilities	In progress
	Consider public subsidies to lower the product certification and service accreditation costs for Australian small to medium enterprises	AustCyber	• AustCyber has recommended that the Federal Government consider additional support for certification and accreditation in the new National Cyber Security Strategy	In progress
	Innovate around procurement processes to identify requirements that can be relaxed for startups and SMEs	Government	• No action to date	Still to be explored

B. Export Australia's cyber security to the world

Target of initiative	Actions listed in 2017	Lead	Actions to-date (non-exhaustive)	Status
Support Australian companies to develop more scalable business models	AustCyber to work with governments to deepen understanding of export opportunities	AustCyber, with government agencies	• AustCyber and Austrade have visited the US, Singapore, Indonesia and Israel to promote Australian cyber exports • AustCyber and the Australian British Chamber of Commerce have visited the UK to promote Australian cyber exports • AustCyber is working with several local firms to develop their global growth strategies	In progress
	Analyse amenability of Australia's existing service strengths to remote delivery of models	AustCyber	• The local ecosystem has seen some consolidation in services (e.g. CyberCX) and growth in education exports	Not yet commenced
	AustCyber to work with governments to map possible target markets for Australian cyber security services and identify potential barriers to export	AustCyber, with government agencies	• AustCyber and Austrade have sent several overseas delegations and are releasing a series of market intelligence reports on overseas market opportunities, including for ASEAN, the US, the UK, and Germany	In progress
	Identify ways to increase scale through partnerships and invest in developing scalable managed service models	Industry, with education and training institutions	• The local ecosystem has made some moves towards scalable models, including strategies that involve overseas partners in the US	Ongoing
Develop cyber security as an educational export	Establish marketing presence in cyber security key target markets and develop partnerships with local businesses that have training needs	Education and training institutions	• AustCyber and Austrade are releasing a series of market intelligence reports which include opportunities around training and skills development needs • AustCyber assists DFAT to carry out their Cyber Capability Engagement Program (CCEP) which aims to build cyber security capacity across the Indo-Pacific, with a strong focus on training cyber security workers and their capabilities	In progress
	AustCyber to work with Australian Government to identify target markets for cyber education exports	Government with AustCyber		In progress
	Promote national security as a national strength within existing Australian education exports, for example Future Unlimited	Government with AustCyber		In progress

Target of initiative	Actions listed in 2017	Lead	Actions to-date (non-exhaustive)	Status
Attract MNCs to use Australia as an export base	Conduct detailed analysis of the existing export benefits of Australian operations of multinational corporations identifying comparative advantage	AustCyber, with government	• There is increasing anecdotal evidence that MNCs are using Australia as an export base, which warrants further analysis	Not yet commenced
	Work with state/territory governments to develop investment incentives for multinational IT companies with cyber security offerings	AustCyber		Discontinued as an action in this SCP

C. Make Australia the leading centre for cyber security education

Target of initiative	Actions listed in 2017	Lead	Actions to-date (non-exhaustive)	Status
Attract the best and brightest to cyber security	Recommendation that AustCyber and other relevant stakeholders work with government/s to expand awareness of cyber security careers in high schools by: • Improving the available information on career paths and role definitions in cyber security • Scaling existing efforts to promote cyber security as a career for women	AustCyber, with government and other relevant stakeholders	• The ACA Schools Cyber Security Challenge and AustCyber's pilot cyber security competition called CyberTaipan, have been launched to spark interest in cyber careers for young people as well as to enhance teacher professional development. Over 30,000 students and 1000 teachers participated in one of these Challenges in 2019 • The Australian Women in Security Network and the Australian Careers Service provide outreach to grow the talent pool	Ongoing
	Increase the number of cyber security scholarships for high school leavers, especially ones that target women and indigenous students	Industry and training institutions	• A series of scholarships for Honours and postgraduate students are available from CSIRO and Data61 as part of the Cyber Security CRC	Ongoing
	Introduce a voluntary 'Digital Nation' program, where post-secondary students gain work experience in digital professions including cyber security	AustCyber, with industry	• No action to date	Discontinued as an action in this SCP

4 BUILDING A COMPETITIVE AUSTRALIAN CYBER SECURITY SECTOR

C. Make Australia the leading centre for cyber security education

Target of initiative	Actions listed in 2017	Lead	Actions to-date (non-exhaustive)	Status
Attract the best and brightest to cyber security	Provide efficient paths for immigration of skilled cyber security professionals by: • Recommending that the Australian Government include ICT Security Specialist to the Skilled Occupation List • Working with training institutions to structure education programs to meet the relevant visas	Government, with training institutions	• The Department of Home Affairs' Global Talent Program has a cyber security focus to attract elite talent who have secured employment within the Australian ecosystem	In progress
	Expand the output and relevance of cyber security programs at Australia's universities and vocational training institutions by working closely with industry in: • Establishing globally compatible core competencies for cyber security degree qualifications that are accepted by both government and the private sector • Seeking opportunities to build significant industry experience component into the curriculum • Supplementing teaching staff with industry personnel and exploring opportunities for this participation to be formally recognised in professional standards • Regularly revising curriculum and course structure to maintain relevance	AustCyber, with training institutions	• Two TAFE cyber security non-degree courses have been developed with industry that students can partly complete on-the-job and are now being offered at TAFEs around the country. Over 2000 students are enrolled in these programs • PWC's Skills for Australia completed a cross sector project in cyber security. This will see eight units of competency in fundamental areas of cyber security available to all students pursuing a qualification in Vocational Education and Training in Australia • Universities are expanding the number and capacity of cyber security education programs and increasingly mapping their curriculum to the NICE Workforce Framework • Academic Centres of Cyber Security Excellence (ACCSE) set up at Edith Cowan University in Western Australia and Melbourne University, with $1.91 million in Commonwealth funding	Ongoing

Target of initiative	Actions listed in 2017	Lead	Actions to-date (non-exhaustive)	Status
Attract the best and brightest to cyber security	Ensure that senior executives, directors and policymakers have access to high-quality cyber security training programs	AustCyber, with industry	• AustCyber, Data61 and the Australian Institute of Company Directors have launched *Cyber for Directors*, a program for senior decision makers to improve their knowledge and understanding of cyber. There are several events each year across Australia • Industry players (e.g. Cybermerc, Fifth Domain and Cyber Aware) have a growing presence as educators and trainers of executives • The Stay Smart Online campaign provides information for business owners to protect their businesses	In progress
	Expand the range of training/ retraining and transitional models available by: • Establishing an apprenticeship model for cyber security that will enable more hiring of graduates • Creating industry-led rapid training/retraining courses to better enable transition to cyber security from other professions	AustCyber, with industry	• Cyber security is part of the Digital Apprenticeship Program run by the Digital Transformation Agency • PwC's Skills for Australia completed a cross sector project in cyber security. This will see eight units of competency in fundamental areas of cyber security available to all students pursuing a qualification in Vocational Education and Training in Australia • The Department of Employment, Skills, Small and Family Business is considering the establishment of a new industry-led Skills Organisation dedicated to Digital Technology and Cyber Security	In progress
	Improve on-the-job training opportunities and clarify career progression options to increase retention and link this to common messaging on the important of cyber security to Australia's national interests	Industry	• Industry awareness of the importance of on-the-job training for both skill development and retention has grown and large organisations are increasing their training offerings • Large firms are beginning to adopt the National Initiative for Cybersecurity Education (NICE) Workforce Framework, a US government taxonomy of cyber security jobs	Ongoing
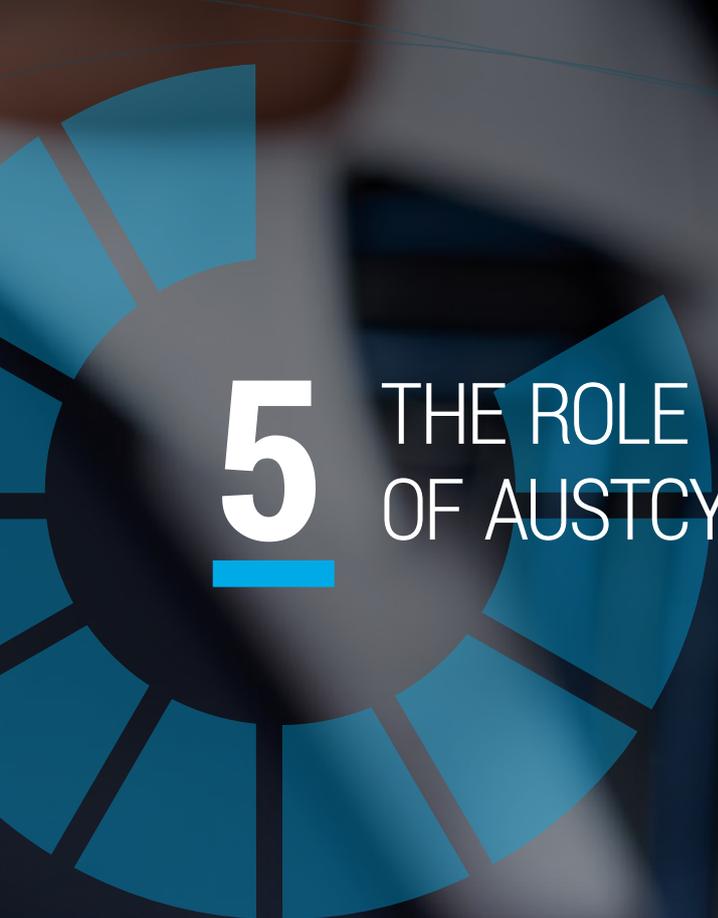
5 THE ROLE OF AUSTCYBER

5.1 ESTABLISHMENT

The Australian Government has recognised the strategic potential of cyber security as part of the nation's security and economic growth. The Government's four-year national Cyber Security Strategy, backed around A$230 million of funding, established the development of Australia's cyber security capability as a national priority issue. This has set Australia on a path to enable all local businesses to grow and prosper through cyber security innovation.

As part of the strategy, AustCyber – the Australian Cyber Security Growth Network Ltd – was formed in 2017 as an independent national body to grow a vibrant and globally competitive cyber security sector.

5.2 ROLE

AustCyber's role is to align disparate cyber security initiatives and investments across the business sector, research community, academia and governments in Australia. Governments play an important part in the cyber security ecosystem. They are as much producers and consumers of cyber security as the private sectors and research community. AustCyber's Co-Chair and Board structures reflect the relevance of governments in the cyber security sector.

> "
> AustCyber's mission is to grow a vibrant and globally competitive cyber security sector that enhances Australia's future economic growth

5.3 MISSION

AustCyber's mission is to grow a vibrant and globally competitive cyber security sector that enhances Australia's future economic growth. As part of this mission, it aims to be an independent national body to better align disparate cyber security initiatives and investments across industry, the research community, academia, and government.

AustCyber is part of the Australian Government's A$250 million **Industry Growth Centres Initiative**, which aims to tap new sources of economic growth by maximising Australia's competitive advantage in six knowledge-driven, high-value sectors. Growth Centres are independent, not-for-profit entities. Each Growth Centre has an industry-led Board, recognising that the private sector is best placed to overcome challenges to innovation, productivity and growth.

Australia's cyber security sector is nascent and, as such, does not currently have strong sector-focused industry associations covering the full breadth and depth of the challenges and opportunities of securing cyberspace. Against this background, AustCyber is working with existing industry groups, such as the Australian Computer Society and the Australian Information Security Association, to ensure a deeper understanding of their ecosystem and policy advocacy opportunities.

AustCyber has quickly cemented relationships with key stakeholders across Australian governments, the private sector and the research community. It is building on relationships to work more closely with other key industry associations and groups, such as the Business Council of Australia, Ai Group, Australian Institute of Company Directors and Council of Small Business Australia. This will help support a more cohesive and vibrant Australian cyber security ecosystem.

AustCyber is led by the needs of the cyber security sector – recognising it as an emerging sector of the economy where business, academia and governments are producers and consumers alike. AustCyber supports Australian-based cyber security businesses from ideation to export. AustCyber has developed a range of mechanisms to enable these businesses to flourish nationally, regionally and globally.

5.4 STRATEGIC THEMES TO MID-2023

Demonstrate leadership and coherence

Create a national cyber security narrative and ensure cohesion across national cyber security programs, leading to accelerated industry investment and more rapid scaling.

Actions: AustCyber continues to raise its public profile, seize opportunities to present its purpose and objectives to stakeholders worldwide, and align the cyber security innovation focus of Australian state and territory governments.

It continues to attend, sponsor and host relevant national and international events, which provide an opportunity to promote AustCyber's unique mission and the world-leading opportunities in Australian cyber security capability.

To strengthen its public image, the Cyber Security Growth Centre rebranded as 'AustCyber' in 2017. It also overhauled its website to include a new section for startups seeking funding opportunities and other relevant information.

AustCyber has started engaging with all Australian, state and territory governments with the goal of signing Memorandums of Understanding with each for a National Network of Cyber Security Innovation Nodes, which are collaborative spaces for cyber security research, innovation and commercialisation.

Drive industry collaboration and coordination

Enable connectivity and information flow to promote high levels of collaboration. This will reduce duplication and therefore allow better leverage of resources and create increased productivity.

Actions: AustCyber has begun to improve the connectivity of the Australian cyber security ecosystem by facilitating meetings and information exchange between businesses and investors.

To better understand how to provide support, it is currently mapping existing activities and gaps in bringing together buyers and vendors of cyber security products and services.

AustCyber continues to host and support events to strengthen the national industry engagement in Australia. For example, in October 2019 it delivered the inaugural Cyber Week nationally.

Accelerate commercialisation

Accelerate the creation and adoption of Australian cyber security products, services and best practices, domestically, regionally and globally.

Actions: AustCyber proactively seizes opportunities to promote Australia's cyber security solutions at key national and international trade shows and summits. It is also working towards increasing the effectiveness of existing Australian incubators and accelerators relevant to cyber security.

In February 2019, AustCyber, in collaboration with Austrade and other key government bodies, led a delegation of almost 50 Australian cyber security companies on a mission to New York, Washington and San Francisco to connect with the world's leading cyber professionals.

To improve the success of Australia's existing incubators and accelerators relevant to cyber, AustCyber has begun to analyse the current R&D landscape and identify gaps in the performance of existing spaces to incubate cyber security startups.

Facilitate talent growth

Rapidly build the size and professionalism of Australia's cyber security workforce to become globally competitive and respected.

Actions: AustCyber is working to address current skills gaps and expand workforce capability through improving workforce education and training, broadening the role of cffyber security challenges, and increasing diversity in the cyber workforce.

In 2017, AustCyber coordinated TAFEs from all states and territories to agree to deliver the first nationally consistent vocational education and training curriculum in cyber security. This started rolling out in 2018. The Certificate IV and Advanced Diploma are based on qualifications developed at Box Hill Institute in Victoria.

AustCyber is developing a comprehensive national program of Cyber Security Challenges, modelled on a UK series of competitions where individuals can test their cyber security skills. These challenges are designed to bolster the national pool of cyber skills by offering activities for individuals to learn and consider a career in the sector.

Pursue policy advocacy and reform

Proactively recommend and support policy and regulatory reforms aimed specifically at the cyber security sector to foster an environment in which innovation and entrepreneurship can thrive.

Actions: AustCyber is working to identify opportunities to harmonise Australian cyber security regulations with international standards to reduce cost of compliance and improve market access. The harmonisation of domestic and international standards to a single globally acceptable standard is a critical step and one that, at the international level, Australia can help progress – leveraging Australia's relative market size to diplomatic and strategic policy standing.

AustCyber is collaborating and consulting with international organisations and key stakeholder groups in Australia to explore opportunities for harmonisation and, where possible, remove bespoke standards and guidance. Where possible, AustCyber seeks to provide improved, tailored communication on regulatory requirements and guidance, with priority for small to medium entities.

Through its policy advocacy role, AustCyber will support industry discussion on issues that may attract regulatory responses and the possible industry impacts of such action, as well facilitate engagement with governments on such discussions.

AustCyber will also work with relevant government agencies to ensure regular industry consultation on export controls and other barriers to cyber security innovation and commercialisation.

AustCyber will further work with industry associations and other peak bodies to ensure industry interests are appropriately represented in discussions on the ways and means to boost the availability of skilled cyber security workers, including on temporary visas and related matters.

AustCyber's Regulatory Reform Plan is at Appendix C.
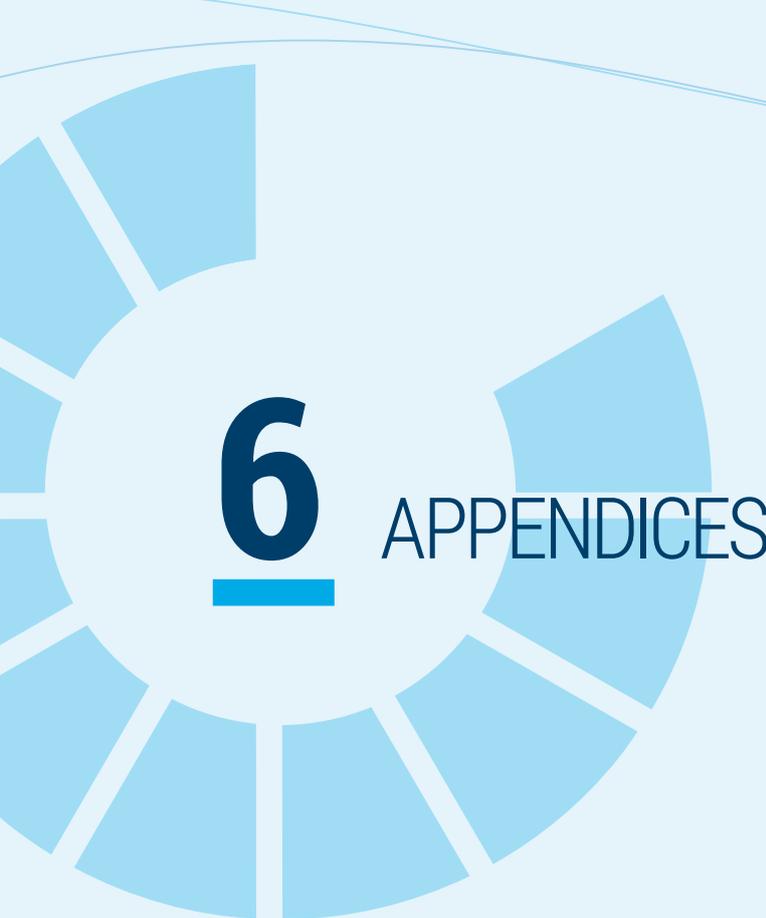
6 APPENDICES

APPENDIX A: INDUSTRY KNOWLEDGE PRIORITIES

Approach to developing knowledge priorities

Knowledge priorities have been developed in line with the current and foreseeable needs and opportunities for industry research and commercialisation in the Australian cyber security sector. They will be used to inform AustCyber's activities as it works with industry and the research community to improve research focus, collaboration and commercialisation performance. This includes engaging with stakeholders in existing cyber security focus areas to develop cyber security capabilities in Data61 and the Defence Science and Technology Group, as well as in universities across Australia. AustCyber will use its nationwide networking expertise to work towards maturing Australia's cyber security ecosystem, and also rely on Data61's existing arrangements with Australian universities on research and commercialisation.

These knowledge priorities for the Australian cyber security have been developed based on a literature review of existing research focuses and consultations with stakeholders as part of the development of this Sector Competitiveness Plan. The major documentary sources are the Australian Government's *Science and Research Priorities* and the CSIRO's report *Enabling Australia's Digital Future: cyber security trends and implications*.[1]

Knowledge priorities

1. **Emerging prevention, detection and response technologies**

   a. *Prevention:* New ways of supporting the nation's cyber security by discovery and understanding of threats, vulnerabilities and opportunities

      i. Being dynamic and proactive with approaches to identifying vulnerabilities, including tools to better predict malicious actor drivers and behaviour

      ii. Prioritising risks in order maximise the value and impact of prevention efforts

      iii. Classifying these vulnerabilities

         1. Exploitation by malicious actors

         2. Non-malicious events such as natural disasters, equipment failure and human error

      iv. From this, developing national resilience, including

         1. Encryption of data

         2. Distributed storage systems that mitigate the impact of a breach

         3. Improved user behaviour

   b. *Detection:* Discovering and assessing intrusions

      i. Determining which technologies can be used to discover intrusions, and developing methods to differentiate this activity from normal human/machine behaviour

      ii. Developing methods to detect a breach even if nothing has been affected yet

      iii. Developing technology to increase the frequency of audits without hampering business activities or incurring significant costs

   c. *Response:* Recovering from a breach

      i. Determining what technologies can be used to remove all known infected systems, applications and devices from the network

      ii. Understanding ways to embed lessons learned for human behaviour and workplace culture

      iii. Increasing the speed at which cyber security breach info is shared across the community

      iv. Ensuring systems continuity, including through self-healing systems

1   Australian Government (2015), *Science and Research Priorities*. Available at: **http://www.science.gov.au/scienceGov/ScienceAndResearchPriorities/Documents/15-49912%20Fact%20sheet%20for%20with%20National%20Science%20and%20Research%20Priorities_4.pdf**.
CSIRO (2014), *Enabling Australia's Digital Future: cyber security trends and implications*.
Available at: **https://www.csiro.au/~/media/Do-Business/Files/CSIRO-Futures/Enabling-Australias-Digital-Future-2014-pdf264MB.pdf**.

2. **Identity, authentication and authorisation in the cyber domain**

    a. Finding new strategies and techniques for systems, applications and individuals to verify, identify and establish trust, including understanding the implications of the abuse of trust

    b. Identifying ways to manage the increasing digital access points (and therefore threat vectors) because of trends toward integrated platforms and mobility

    c. Identifying the best use of advanced sensors/ intelligent devices to verify trust

3   **Ensuring security, privacy, trust and ethical use of emerging technologies and services such as**

    a. Cloud computing

    b. Cyber-physical systems, including the Internet of Things, robotics, self-driving cars etc.

    c. Machine learning

    d. Big data and data analytics

    e. Mobile applications

4   **Approaches to deal with the increasingly 'shared' responsibility of cyber security**

    a. Developing a better understanding of user behaviour at the macro level (including norms of behaviour in cyberspace and user interaction with integrated platforms) and its impact on cyber security

    b. Ensuring the evolution in cyber security policies and skills closely match changes in technology, our adoption and then dependence

    c. Creating a culture with a deeper understanding of cyber security challenges and breaches, including the importance of information sharing, recognising the interdependence of cyber security with national security, national interest and economic prosperity

APPENDIX B: METHODOLOGIES AND ASSUMPTIONS

Industry revenue

At present there are significant measurement challenges in estimating cyber security revenues in Australia. Cyber security is not captured by Australian Bureau of Statistics industry definitions. It is therefore necessary to use external market research estimates (a range of divergent estimates exists) and assumptions to form a view on the amount of revenue that accrues to cyber security providers in Australia. The demand and revenue figures presented in this report should be interpreted as estimates only and a wide confidence interval should be applied when using them to inform decision-making.

To estimate industry revenue by segment and the share of demand currently met by Australian companies, a proprietary model was built based on a range of data sources, including Gartner and IDC.[2] The assumptions for market shares (that is, share of Australian spend) and export shares (proportion of revenues that are derived from exports) for Australian companies are shown in Figure 52, as well as the source of those assumptions.

---

2   Market size by country obtained from Gartner (2016), *Information Security, Worldwide, 2014–2020, 3Q16 Update* and combined with similar estimates from IDC and IbisWorld; software market share data obtained from IDC (via custom data requests).

Figure 52

Assumptions used in estimating Australian cyber security revenue

Market share assumptions

Share of Australian market by type of firm % of Australian cyber security spend		Initial SCP*	This update	Source/rationale
Hardware	Domestic players	5%	6%	Estimate based on conversations with IDC, and analysis of domestic market share by provider
	Foreign players with core business in Australia	0%	0%	Core business (i.e. design) is typically kept in the home jurisdiction
	Foreign players with sales team only	65%	64%	Foreign product firms in Australia typically have a sales team only
	Foreign players with no presence	30%	30%	Interview with IDC (70% of firms serving Australian customers have an Australian office)
Software	Domestic players	5%	6%	Estimate based on conversations with IDC, and analysis of domestic market share by provider
	Foreign players with core business in Australia	0%	0%	Core business (i.e. software development) is typically kept In the home jurisdiction
	Foreign players with sales team only	65%	64%	Foreign product firms in Australia typically have a sales team only
	Foreign players with no presence	30%	30%	Interview with IDC (70% of firms serving Australian customers have an Australian office)
Services	Domestic players	25%	27%	Team judgment, based on evidence from interviews (international services players receive much more attention)
	Foreign players with core business in Australia	50%	50%	
	Foreign players with sales team only	20%	18%	While a large services player will typically have more than a sales team in Australia (indicating a larger weight), some firms outsource their SOCs to low-cost countries (we therefore applied a penalty)
	Foreign players with no presence	5%	3%	Assumed to be low as it is difficult to provide services with no in-country presence

1
2

Export assumptions

Exports as a % of revenue by type of firm % of firm revenue		Initial SCP*	This update	Source/rationale
Hardware **Software**	Domestic players†	66%	68%	Interviews with industry players combined with team judgment
Services	Domestic players	10%	10%	Interviews with stakeholders, which suggest few services firms are currently exporting from Australia
	Foreign players with core business in Australia	10%	10%	

3

* The 'Initial SCP' assumptions are still applied to 2016 and prior years' data (updated assumptions apply from 2017 onwards)

† Export assumptions were not required for 'foreign players with core business in Australia' as this group was assigned a zero market share for software and hardware.

SOURCE: Expert & stakeholder interviews, UN World Input-Output tables, team analysis

1   Recent stakeholder conversations suggested that Australian home-grown software and hardware firms have begun to experience increased success in securing first contacts. While this effect is still nascent, the market share of home-grown hardware and software firms was increased slightly to reflect this.

2   Industry stakeholders in the cyber security industry noted strong revenue growth over the past year (beyond what market research data suggested). The market share of domestic service firms was increased slightly to reflect this.

3   The export share of revenue for Australian cyber security software and hardware players was increased slightly to reflect their continued international growth.

Workforce supply shortage and economic costs

In this Sector Competitiveness Plan, a skills shortage is defined as the additional number of workers that would be in the core cyber workforce if the supply of suitable workers were unconstrained (see Figure 53). Suitable workers have both the technical and non-technical (for example, communication skills) skills that employers consider important.

Figure 53

Modelling demand and supply of cyber security workers

Total costs of different cyber training programs
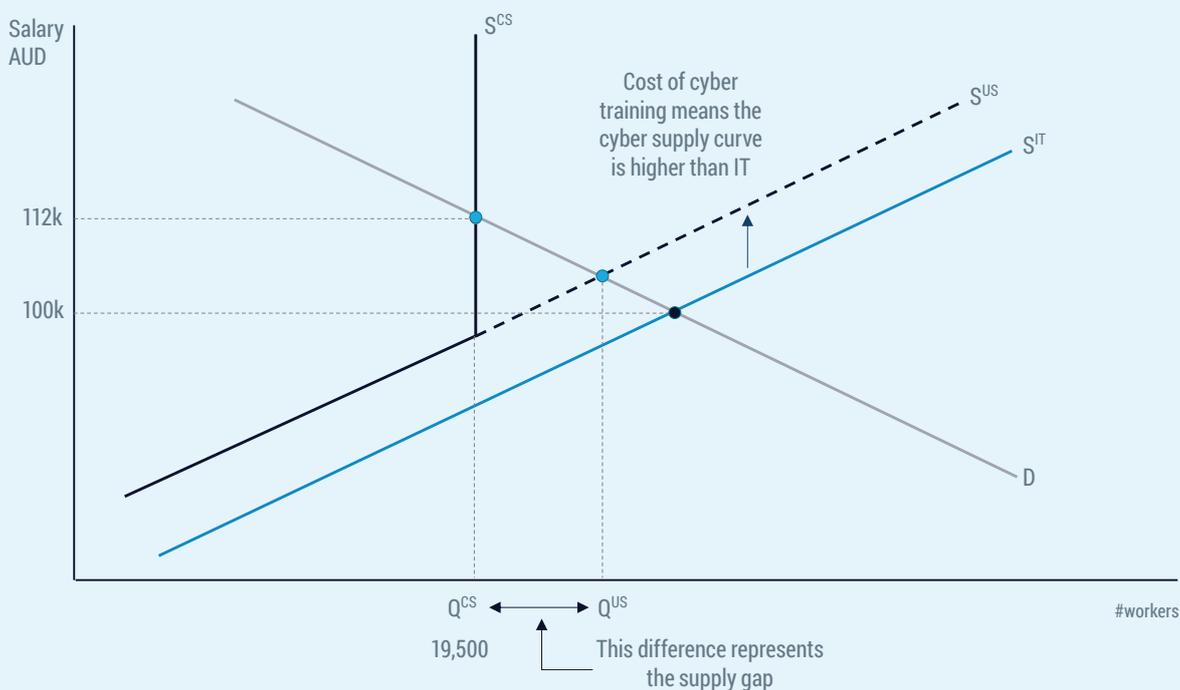
Comments

- Currently the supply of cyber workers is constrained, as shown by the black line S^{CS}

- IT is a relatively unconstrained industry because of its large size, and its pool of potential workers. Its supply of workers is represented by the blue line S^{IT}

- Using IT as a benchmark, and factoring in the cost of specialised cyber security training, the unconstrained supply of cyber workers is given by the dashed black line S^{US}

- The cyber workforce supply gap is the difference between Q^{CS} and Q^{US}, the additional workers that would be in cyber if there were no supply constraint.

SOURCE: Gartner, ABS, AlphaBeta Analysis

Estimating the current workforce supply gap is difficult. As such, four different approaches based on job market metrics were used: the wage premium; recruitment failure rates; recruitment time; and job market depth (see Figure 22 for details on the four metrics).

Wage premium: IT was used as a relatively unconstrained industry. Assuming a unitary elastic demand curve, the IT salary plus cyber training costs was mapped to the demand curve to derive the unconstrained cyber workforce size. The process is illustrated in Figure 53.

Recruitment failure rate: The number of unfilled cyber jobs was estimated by taking the number of cyber job ads and assuming that the recruitment failure rate for cyber was equal to IT overall and the best performing IT category for recruitment success.

Recruitment time: The number vacancies that could have been advertised if cyber security's time to fill were equal to IT was calculated using the number of cyber job ads and time to fill in cyber and IT. The difference between these estimates represents the workers that would have been in the cyber workforce had supply been unconstrained.

Job market depth: The ratio of the number employed over the number of job ads was calculated for cyber, IT, and the national average across industries. The size of the workforce that would be required in cyber align cyber security's job market depth with the latter two benchmarks was then calculated.

Using the output of these four analyses, the minimum and maximum estimates across the metrics were taken as the supply shortage range. Note that job market data does not account for unadvertised cyber roles (for example, some cyber roles in the Defence Force). This means the supply shortage could be even larger.

Financial impacts of the skills shortage were calculated based on the average revenue or wages per worker in the cyber sector. This is because the skills shortage reduces both the revenue of cyber security providers, and the wages paid to internal cyber security teams within cyber users.

APPENDIX C: REGULATORY REFORM PLAN

Digital trade – and efforts to secure it – is a mainstay of the global economy. The point of difference to traditional forms of trade is that it occurs in cyberspace, a conceptually borderless domain of human interaction. Observing other more cyber mature economies, it is clear that disparate national approaches to the regulation and standardisation of cyber security pose significant barriers to efficient trade relationships and effective innovation.

Domestically, Australia is in a nascent stage of regulation on cyber security. Australia's **Cyber Security Strategy** identified that existing regulations are sufficient to encourage good risk management practices and foster innovation. The Cyber Security Strategy also identified that existing voluntary standards, as a means of self-regulation, are appropriate for Australia's current (comparatively low) level of cyber maturity. The work undertaken to develop the Cyber Security Sector Competitiveness Plan supports the Strategy's position.

However, the following areas for optimisation have been identified as supporting support industry growth and the economy as it embraces cyber security and develops innovative solutions to cyber challenges:

- harmonisation of cyber security regulatory and legislative frameworks both domestically and internationally, industry self-imposed regulations, standards and guidance;

- active discussion on issues which may attract regulatory responses and industry impacts of such action;

- engagement in strategic discussions with relevant agencies on implications of the applicable multilateral export control regime, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies; and

- access to skilled labour, specifically through temporary visa arrangements.

Cyber security is a global industry and a globalised endeavour. Australian public and private sector entities as well as academic institutions and non-profits are required to navigate multiple national and international standards and guidance. This affects industry productivity (as well as public sector efficiency), can be cost prohibitive for small entities to engage in some markets, and can inhibit access to global export markets. The harmonisation of domestic and international standards to a single globally acceptable standard is a critical step and one that at the international level, Australia can help progress, leveraging our relative market size to diplomatic and strategic policy standing.

As the Australian economy becomes increasingly mature in its management of cyber risk and embedding cyber resilience, it will be increasingly important to be mindful of regulatory duplication, inconsistencies and inefficient complexity. Proactively working toward regulatory harmonisation, including self-regulation, will support good practices and help encourage innovation and flexibility.

Where regulation is deemed to be necessary, Australia should work to ensure the focus is on risk based and outcome-focused regulation. This requires strong demonstration of performance but allows for ecosystem development and changing environments.

Standardisation is also recognised as a key factor in the Australian Government's Innovation and Competitiveness Agenda released in 2014, with alignment to international standards set to deliver significant competitiveness, productivity and efficiency gains to the Australian supply chain.

Action

Australia should seek to adopt trusted international standards and review regulations to remove references to local bespoke standards, including differences in standards and guidance between domestic jurisdictions. Regulations may need to bridge any gaps between international standards and standards required for genuinely local conditions. Australian entities should use standards to enhance technical integrity, improve risk management practices, enable cost effective investment in security and encourage innovation. Aligning with international standards also facilitates local industry to compete in global markets and attracts sustained foreign investment.

AustCyber will work, in partnership with key stakeholders, to explore opportunities for harmonisation and, where possible, remove bespoke standards and guidance. This will include working with international organisations and consulting broadly across stakeholder groups in the Australian economy. AustCyber will also work with these stakeholders to provide improved, tailored communication on regulatory requirements and guidance, with priority for small to medium entities.

Through its policy advocacy role, AustCyber will support industry discussion on issues, which may attract regulatory responses and the possible industry impacts of such action as well facilitate engagement with governments on such discussions (refer to AustCyber's Business Plan).

Technology-based cyber security solutions are part of a growing set of technologies that can be applied to lawful and unlawful activities, as well as in nation-state escalatory behaviour (pre-war and war). That is, they have 'dual use'. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, of which Australia is a signatory, applies in these circumstances, mainly impacting solutions incorporating cryptographic technologies.

As cyber security solutions and new technologies evolve, it is increasingly important to consider their dual uses and appreciate the possible positive and negative impacts of globally mandated export controls on the innovation process. It is critical industry engagement on these impacts is included in governmental efforts to comply with and evolve the Wassenaar Arrangement and similar international regimes and conventions.

Action

AustCyber will work with relevant agencies within the Australian Government to ensure regular industry consultation on the barriers and benefits to cyber security innovation and commercialisation of export controls and similar international regimes and conventions. AustCyber will also support efforts for the translation of international policy agreements into domestic regulatory and self-regulatory frameworks.

The Sector Competitiveness Plan confirms the position described in Australia's Cyber Security Strategy, that the Australian economy has an extant shortage of skilled cyber security labour, forecast to worsen without intervention. The Sector Competitiveness Plan is one source of action to address this challenge, as is the Cyber Security Strategy, AustCyber's Business Plan and a wide range of other government and corporate action.

As the skills pipeline issues are addressed and the size of the cyber security workforce increases, it will also be important to support labour mobility within Australia and globally, to ensure the ecosystem develops in ways that incorporate the most advanced thinking and solutions development. This will require the sector to engage in, among other policy related activities, debates on the modernisation of Australia's skilled migration policy.

Action

AustCyber will work with industry associations and other peak bodies to ensure industry interests are appropriately represented in discussions on the ways and means to boost the availability of skilled cyber security workers, including on temporary visas and related matters.

"

AustCyber's mission is to grow a vibrant and globally competitive cyber security sector that enhances Australia's future economic growth.

Contact

Email: info@austcyber.com

Phone: 0455 260 848

Website: www.austcyber.com

Twitter: @AustCyber

Office: Suite 3, Level 3
           1 Franklin Street
           Manuka ACT 2603

Australian Government
Department of Industry, Science, Energy and Resources

Industry Growth Centres

AustCyber
Australian Cyber Security Growth Network