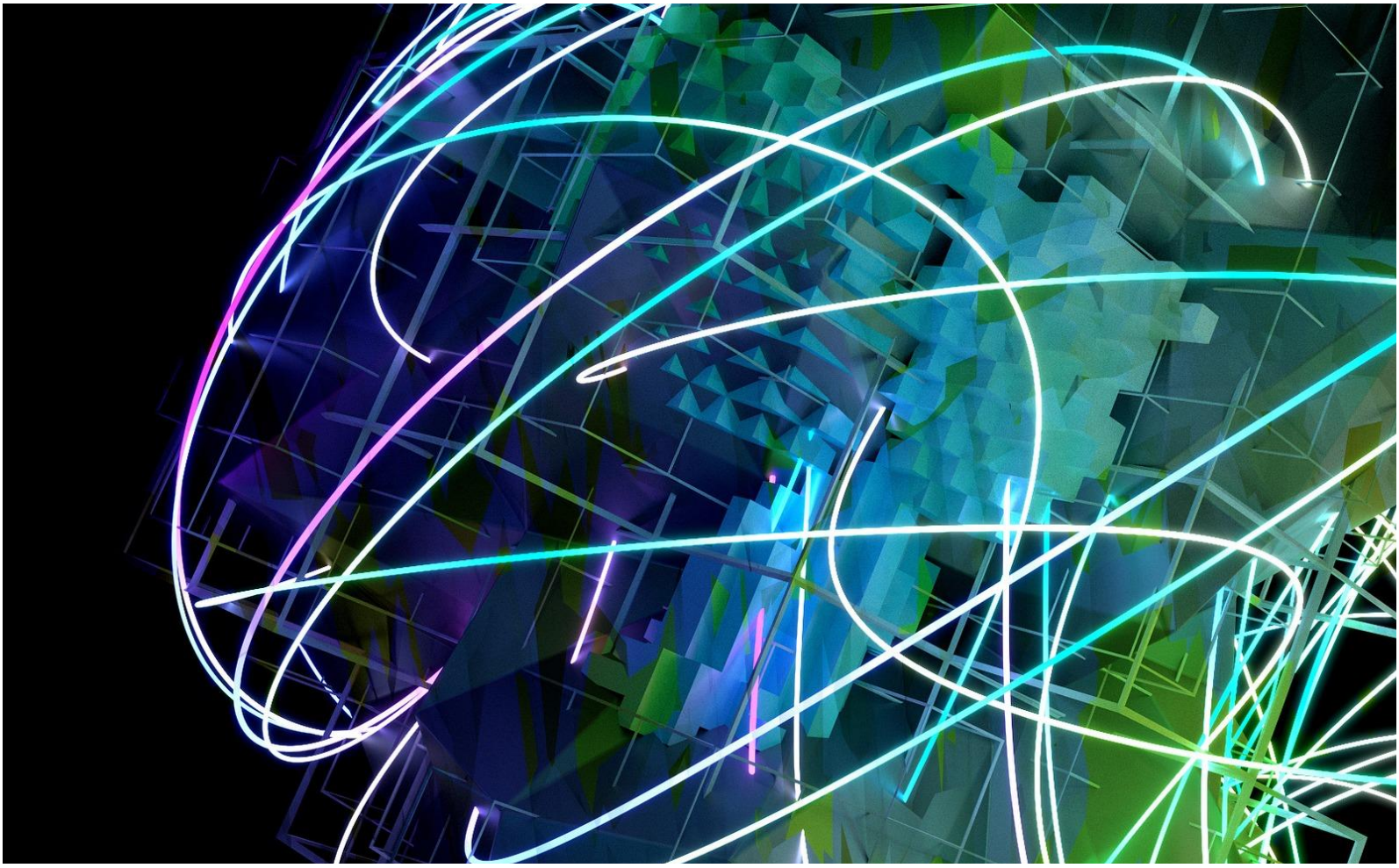


Cyber Security Sector Competitiveness Plan

Australian Cyber Security Growth Network

April 2017

Table of Contents

Preface 2

Acknowledgements 4

Executive summary 1

1. The global outlook for cyber security 5

1.1 Overview 5

1.2 Cyber security is a fast-growing industry 5

1.3 Three basic security needs shape demand for different cyber security product types 8

1.4 Technology is reshaping the industry 14

2. The potential of Australia's cyber security industry 17

2.1 Overview 17

2.2 Local demand is strong, especially for services 18

2.3 Supply is dominated by imports 19

2.4 Australian firms have existing strengths in software and services 21

2.5 Australia's opportunity: focus initially on a limited number of segments 24

2.6 Playing to our industry strengths 29

2.7 The size of the prize: benefits for Australia 31

3. Challenges to Australia's cyber security industry 34

3.1 Overview 34

3.2 Research and commercialisation 35

3.3 Firm growth and export 49

3.4 Skills and workforce 61

4. Building a competitive Australian industry 73

4.1 Grow an Australian cyber security ecosystem 73

4.2 Export Australia's cyber security to the world 79

4.3 Make Australia the leading centre for cyber security education 82

4.4 Summary of strategies and actions 86

5. The role of ACSGN 88

Appendix A: Industry Knowledge Priorities 90

Appendix B: Methodologies and assumptions 92

Preface

Cyber security is now one of the most rapidly expanding industries globally, as governments, the private sector and research community have begun to boost their spending and investment in an effort to fend off perpetrators of malicious cyber activities. Further, trust and confidence in a cyber secure economy paves the way for enhanced growth as the world seeks out new economic opportunities in the interface between physical and virtual domains.

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 by adversaries to steal secrets and other information stored in a digital format 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 be a front-of-mind issue for business leaders, regulators and politicians who are anxious to shore up defences and improve resilience.

The growing demand for cyber security products and services provides a significant economic opportunity for Australia. Australia's growth prospects are sizeable if it succeeds in focusing on the unique strengths and advantages it possesses in cyber security. This is true even though the domestic cyber security sector is still in its infancy and the Australian market has so far been dominated by foreign players.

The role of the Australian Cyber Security Growth Network Ltd (ACSGN) is to set the direction for Australia's cyber security industry to advance and prosper and offer a trusted source of cyber security capability to organisations at home and abroad. ACSGN is part of the Australian Government's A$250 million Industry Growth Centres Initiative, which aims at tapping new sources of economic growth by maximising Australia's competitive advantage in six knowledge-driven, high-value sectors. Growth Centres are enabling organisations to become more innovative, collaborative and export-focused. They are improving commercialisation pathways and link great solutions with global supply chains, while enhancing workforce skills and shaping regulatory reform. ACSGN is also a key initiative of Australia's Cyber Security Strategy, which identifies that cyber security growth and innovation is as important to Australia's cyber security posture as tackling cyber threats.

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. In the case of cyber security, Australian governments are as important to the development of the industry as the private sector and the research community – they too are consumers of cyber security products and services and major employers.

Based on a wide range of interviews with the private sector, policymakers and researchers (see Acknowledgements), ACSGN has developed a Sector Competitiveness Plan (SCP) to identify the challenges Australian organisations face when competing in local and international cyber security markets. The SCP provides a roadmap to strengthen Australia's cyber security industry and pave the way for a vibrant and innovative ecosystem. It articulates the steps and actions required to help Australia become a global leader in cyber security solutions, with the aim of generating increased investment and jobs for the Australian economy.

Acknowledgements

The ACSGN gratefully acknowledges the following companies, industry associations, government bodies, research institutions and universities for their valuable input into the Sector Competitiveness Plan, and the participation of individuals from many of these organisations in the AlphaBeta/ McKinsey survey of CIOs, CISOs and cyber security providers that supported the development of this Plan. These organisations have not endorsed the contents of this plan.

AGC Partners
Amadeus Capital Partners
Austrade, Australian Government
Australia Defence Force Academy / UNSW Canberra
Australian Federal Police, Australian Government
Australian Information Security Association
Australian Signals Directorate, Australian Government
Australian Unity
CERT Australia, Australian Government
Cisco Systems
Coles Supermarkets
Commonwealth Bank of Australia
Data61
Deakin University
Decipher Bureau
Defence Science and Technology Group, Australian Government
Department of the Prime Minister and Cabinet, Australian Government
Department of Industry, Innovation and Science, Australian Government
Edith Cowan University
Hivint
IBM
icare
Intelligent Business Research Services
Kasada
KPMG
La Trobe University
Macquarie Telecom
Medibank Private
Nuix
Optus
QuintessenceLabs
Secure Code Warrior
Security Innovation Network
Westpac

The ACSGN also gratefully acknowledges Nuix, penten, ResponSight, Airlock Digital, Cog Systems, QuintessenceLabs, FunCaptcha, Bugcrowd, Dtex Systems and Upguard for their contributions to various case studies featured in this plan.

The development of this Plan was also informed by the extensive consultations with governments, the private sector and the research community within Australia and internationally, undertaken by the Department of the Prime Minister and Cabinet as part of the development of Australia's Cyber Security Strategy; and by the Department of Industry, Innovation and Science as part of the establishment of ACSGN.

Executive summary

Australia is well placed to become a global cyber security powerhouse. Its promising strength in core research areas like quantum computation and secure third-generation microkernel, its well-developed services economy and the quality of its education system make it an ideal growth environment for organisations offering innovative cyber security solutions. While cyber security is a nascent industry in Australia, this report shows that favourable market conditions and concerted efforts could lead to tremendous growth. Over the next decade, the Australian cyber security industry has the potential to almost triple in size, with revenues soaring to A$6 billion by 2026, from just over A$2 billion today (Exhibit 14 refers).

Underpinning this attractive outlook are expectations that demand for cyber security will increase dramatically in coming years—particularly in the Indo-Pacific region—as cyber criminals are becoming ever-more astute in their malicious activities, emboldened by the growing number of electronic devices they can target in an ever-more connected world. In response, the cyber security industry will become larger, more diverse and more sophisticated in servicing the security needs of organisations concerned with managing their cyber risks.

Recognising that strong cyber security is a foundation for economic growth and prosperity, the Australian Government last year launched its national Cyber Security Strategy, which elevated cyber security as an issue of national importance. The strategy, backed by around A$230 million of funding, made strengthening the local cyber security industry one of five areas of priority action to support sovereign capability development and ensure Australia takes advantage of the significant economic opportunities in the global cyber security market. It includes several initiatives designed to enable cyber security innovation, support the development of new cyber security businesses, promote the export of Australian cyber security products and services and ensure cyber security research and development meets industry needs.

The key initiative to this effect is the creation of a Cyber Security Growth Centre. The role of the Australian Cyber Security Growth Network Ltd (ACSGN)—the publicly funded private entity that is the Cyber Security Growth Centre—is to set the direction for Australia's cyber security industry to advance and prosper and offer a trusted source of cyber security capability to organisations at home and abroad. ACSGN is also part of the Australian Government's A$250 million Industry Growth Centres Initiative, which aims at tapping new sources of economic growth by maximising Australia's competitive advantage in six knowledge-driven, high-value sectors and enabling organisations to become more innovative, collaborative and export-focused.

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. In the case of cyber security, Australian governments are as important as the private sector and the research community in the development of the industry—they too are consumers of cyber security products and services and major employers.

Australian cyber security businesses are operating in a highly competitive and fast-evolving global market, in which US-based firms have so far met the bulk of demand. Their efforts to become more relevant, more competitive and more successful on the world stage are further complicated by three country-specific challenges.

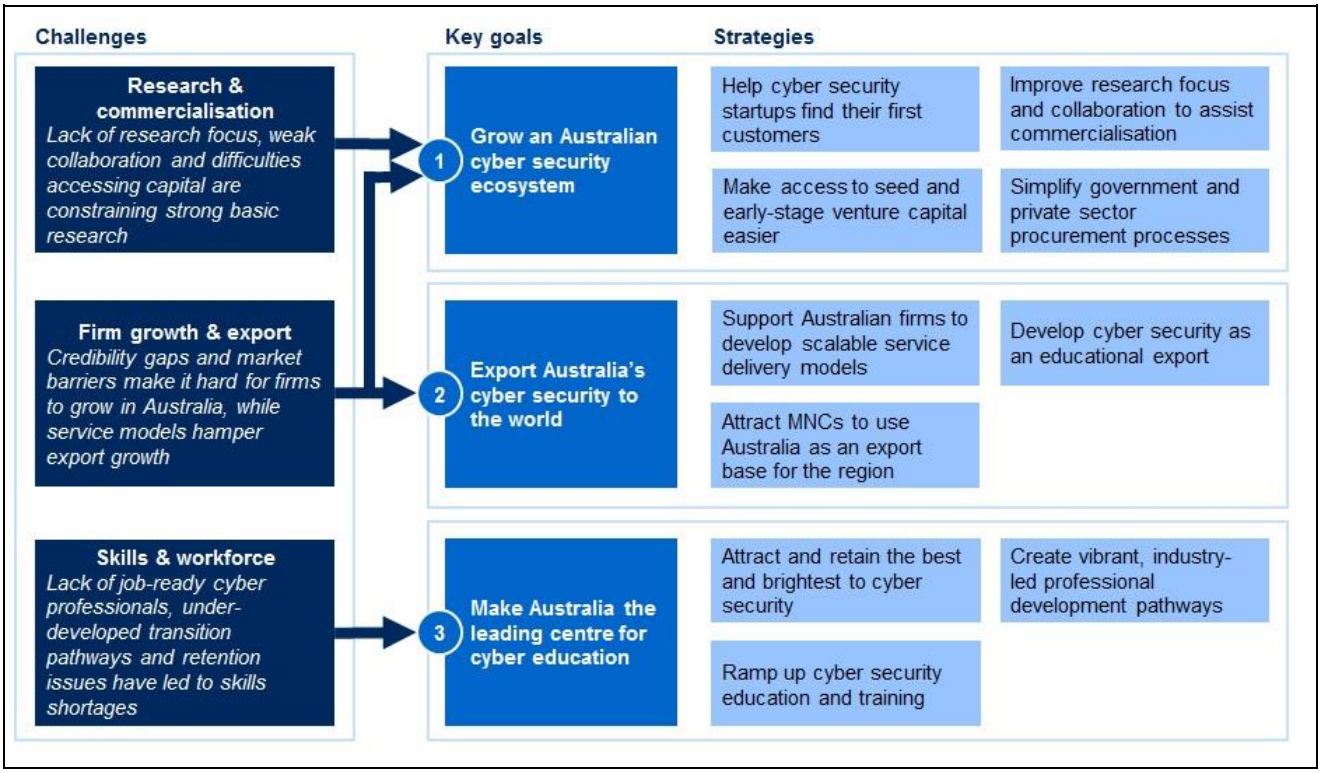
Firstly, while Australia demonstrates excellent and world-leading cyber security research capability, there are signs the current system of research and commercialisation is inefficient. Scattered public funding for cyber security research and development weakens the country's ability to lead on innovation. Limited collaboration between the research community and the private sector further undermines the commercialisation of basic research ideas into marketable solutions.

Secondly, insights gained from expert interviews undertaken to develop this Plan and public tender data signal that the current market environment constrains the growth prospects of smaller Australian cyber security businesses and startups. While these companies may have the capability to develop innovative and novel product and service offerings, they often lack the business acumen, established credibility and scale to win key contracts with large industry or government customers in Australia and abroad. Barriers to export are particularly noticeable for providers of cyber security services.

Thirdly, a serious skills shortage is limiting the growth of the Australian cyber security industry. Several industry surveys confirm the drought in job-ready cyber security professionals is among the worst in the world. While universities have recently begun to introduce several new study courses, they will unlikely produce enough graduates to meet industry demand in the near future. It is also questionable whether the industry will be able to draw workers with related skills from areas outside of cyber, as pathways for professional and transitional training are not currently sufficient. It is estimated that the domestic cyber security industry will need to employ at least 11,000 additional workers over the next decade.

ACSGN has produced this Sector Competitiveness Plan (SCP) to analyse these three challenges, to deepen the understanding of the local and global cyber security industry and its participants, and to offer strategies and actions that Australian governments, the private sector, training and research institutions, and ACSGN itself, can undertake to foster the growth of Australia's cyber security industry. Exhibit 1 provides an overview of the key elements of the SCP. The SCP has a 10-year outlook. However, given the rapid evolution of the cyber domain, the plan will be revised annually by ACSGN to take account of changing technology, market conditions and progress to date.

Exhibit 1:



The report's findings are laid out over five chapters. Chapter 1 provides an overview of the composition and size of the global cyber security industry. It outlines the key demand forecasts that are underpinning the cyber security industry's rapid growth. This chapter also investigates how major technological trends, from Big Data to the Internet of Things, are set to shape the future pattern of demand across the industry's key segments.

For the Australian cyber security industry, the growth opportunity is large. As Chapter 2 describes, the market appears particularly buoyant for service providers. In Australia, where the vast majority of public and private sector organisations lack the capacity to employ large internal cyber security teams, demand for external cyber services is already stronger than elsewhere in the world—and this situation will likely intensify in the future.

So how can Australia use its country-specific advantages to increase the competitiveness of its cyber security industry? While examples of globally successful Australian cyber security firms can be found in hardware, software and services, three market segments stand out as particularly attractive: software; services to improve security of basic IT and network infrastructure; and services focussed on underlying processes, such as governance, risk and compliance, and training and awareness. The analysis outlined in Chapter 2 suggests that these three market areas currently promise the steepest economic gains and should therefore be treated as initial focus segments that warrant priority action.

The report then provides an overview of three key issues holding back the Australian cyber security industry's growth and innovation power. Chapter 3 takes a detailed look at blockages in the national research and commercialisation system for cyber security; it describes the market barriers that make it difficult for smaller cyber security firms to become global export-focused players; and analyses the skills shortage currently gripping the industry.

But these challenges can be overcome with targeted, concerted policy action. Chapter 4 makes a range of policy recommendations against the three key goals of this plan and is designed to complement and enrich the existing initiatives outlined in Australia's Cyber Security Strategy.

ACSGN recognises the development of a highly capable and globally competitive cyber security industry in Australia must be led by industry itself, with strong support from research and training institutions and Australian governments. Chapter 5 provides more details on the specific role ACSGN intends to play to enable this success.

This SCP also includes the articulation of Industry Knowledge Priorities (Appendix A), which set out the industry research needs and commercialisation opportunities for Australia's cyber security industry. The knowledge priorities will be used to inform the activities of ACSGN as it works with stakeholders across the economy to improve the industry's research focus, collaboration and commercialisation outcomes.

Future versions of the SCP will include a Sector Regulation Reform Agenda that will identify any further need for regulation in the domestic cyber security industry, including reform opportunities within the remit of the Australian Government. This will build on the work undertaken by the Government through the 2015 Cyber Security Review (resulting in Australia's Cyber Security Strategy), which considered existing regulatory mechanisms were sufficient given the current level of maturity of cyber security and cyber risk management.

The goal of the SCP's action plan, whose key points are summarised in Exhibit 1, is to strengthen Australia's cyber security ecosystem and help Australia become a powerful cyber security exporter and world-leading cyber security education hub.

1. The global outlook for cyber security

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.

Cyber adversaries are constantly contriving new ways to exploit vulnerable systems and networks, thus forcing organisations—from banks to energy companies, from government agencies to charities—to strengthen their cyber defences. The growing security needs of these organisations are expected to underpin the rapid growth and evolution of the global cyber security industry over the next decade. Global spending on cyber security is expected to almost double by 2026, from around US$126 billion today, as shown in Exhibit 2. This surge in demand provides a substantial growth opportunity for cyber security businesses in Australia and elsewhere.

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

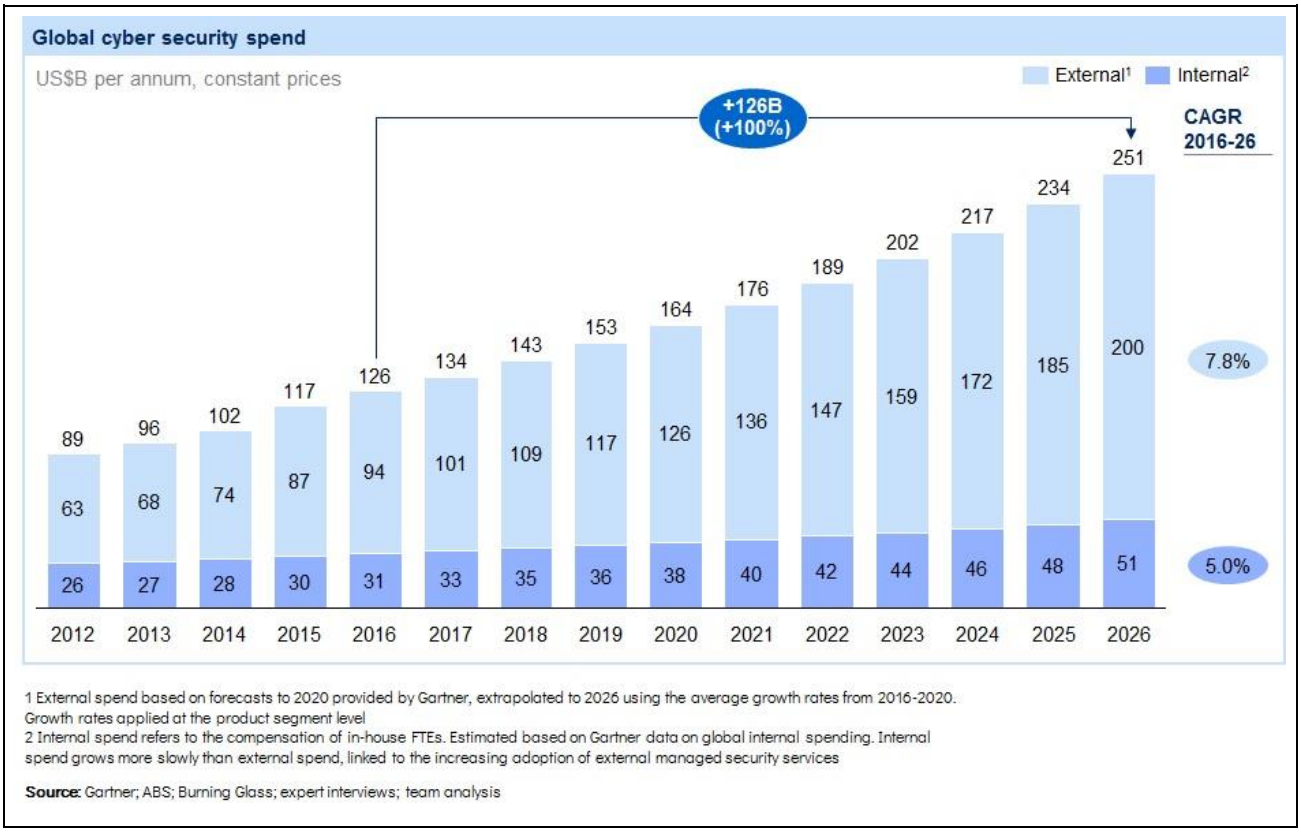
The Internet of Things, Cloud Computing and the convergence of IT and operational technology (OT), are some of the current important disruptive technological trends that will contribute to the future demand of cyber security solutions. They will increase demand for all forms of cyber security, particularly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

1.2 Cyber security is a fast-growing industry

The global cyber security market is currently worth around US$126 billion and is projected to roughly double to US$251 billion over the next decade, as shown in Exhibit 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) who purchase the products and services of *external* cyber security 'providers' (both specialist cyber security firms and IT or telecommunications firms with cyber security offerings). The remaining quarter is the *internal* expenditure of cyber security users on their in-house capabilities, principally wages of their IT staff who specialise in cyber security.[1]

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

Exhibit 2:



1 External spend based on forecasts to 2020 provided by Gartner, extrapolated to 2026 using the average growth rates from 2016-2020. Growth rates applied at the product segment level
2 Internal spend refers to the compensation of in-house FTEs. 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; ABS; Burning Glass; expert interviews; team analysis

Growing security threats and sophistication of attackers are driving demand

Several trends are supporting the growth outlook:

- **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, an average client of technology company IBM Corporation experienced 178 security incidents in 2015, 64 per cent more than in the previous year.[2] Software provider Symantec Corporation discovered more than 430 million new unique pieces of malware in 2015, up 36 per cent from the year before. The frequency of so-called mega breaches, defined as the loss or theft of over ten million personal data records at once, has soared to record highs globally.[3] But official numbers likely only represent the tip of the iceberg, as more and more companies choose not to reveal the full extent

of the data breaches they experience. Symantec estimates the true number of lost records to be closer to half a billion. Cyber threats have increased markedly in Australia, too. Between July 2015 and June 2016, CERT Australia—the national Computer Emergency Response Team—responded to 14,804 cyber security incidents in Australian businesses, 34 per cent more than in the twelve months prior, according to recent threat reports by the Australian Cyber Security Centre.[4] Energy and financial services companies were the most affected. Meantime, the Australian Signals Directorate responded to 37 per cent more government cyber security incidents in 2014 compared to previous years.[5]

- Mounting exposure to cyber risk – The rapid expansion of Internet-enabled economic activity and the number of connected devices and systems increase the certainty of widespread malicious cyber activity. People in far corners of the globe are gaining online access, as the world is becoming more digitalised and interconnected. This is partly attributable to smartphone penetration, which has risen remarkably 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. A recent survey by Telstra shows that executives across every business sector in Australia are now concerned about cyber security.[6] A majority of executives are briefed at least quarterly on cyber risks and mitigation strategies. The survey also reveals that cyber security programs are increasingly seen as a "boardroom issue". In 35 per cent of companies surveyed across Asia, cyber security programs are dealt with by top-level executives and board members, although the number is still significantly lower (at around 19 per cent) in Australia.

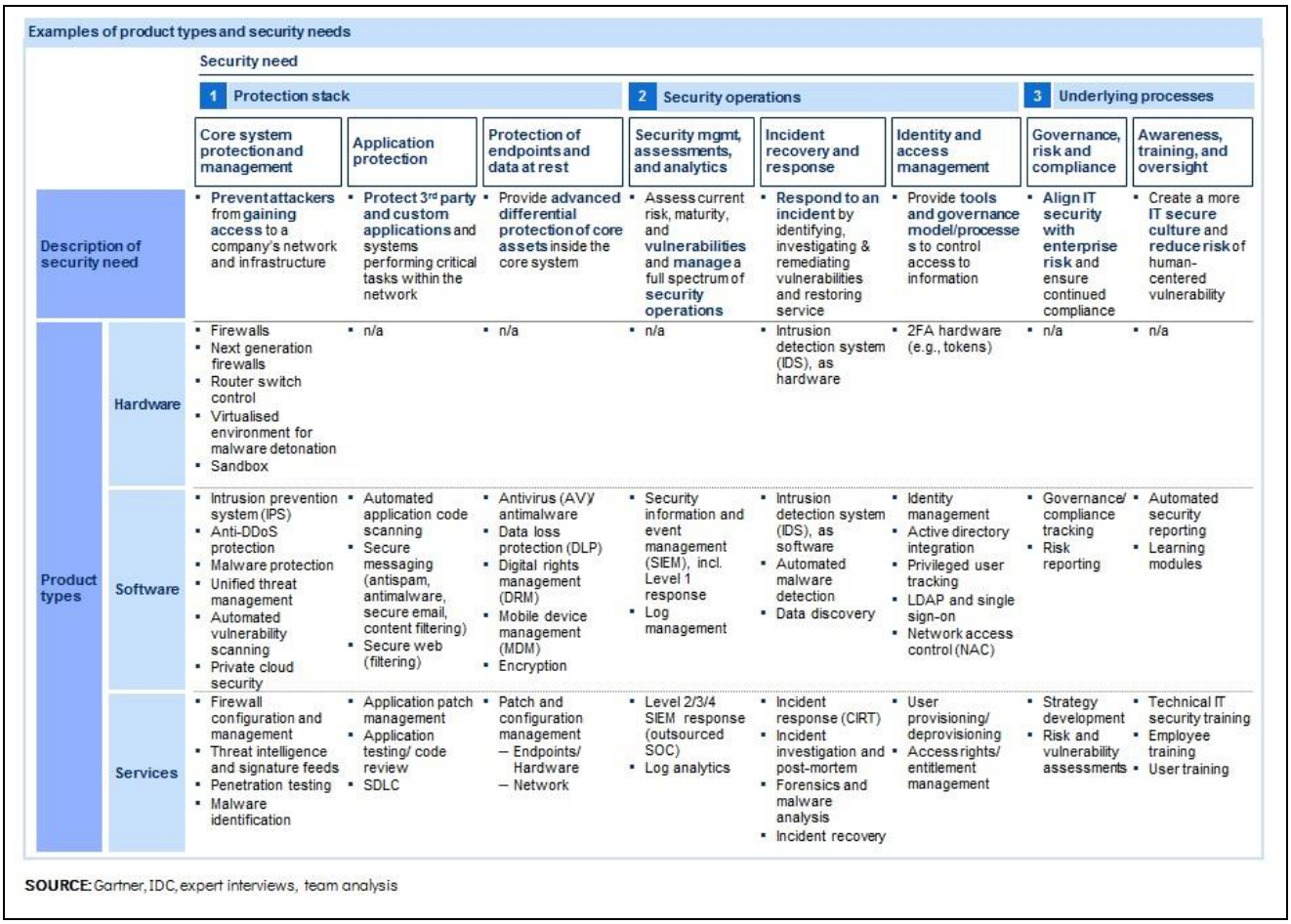
- Increasing regulation of cyber risk – Governments of many countries are seeking to bolster their national defences against cyber attacks and other malicious cyber activity, and they are increasingly concerned about the cyber defences of sectors within their economies. Many governments worldwide have begun to issue new laws and regulations to ensure confidential information remains secure. These new regulations challenge organisations to have the right cyber security controls in place and will likely entail further security spending. For example, regulatory oversight has forced banks and insurance firms to be acutely aware of malicious cyber activity threatening their operations. The Australian Prudential Regulation Authority (APRA) obliges board members and executives to fully understand current cyber security risks and expects them to be well-informed in relation to their organisation's ability to prevent, detect and respond to any attack. The result: 85 per cent of boards or board committees in the Australian financial industry are now receiving periodic updates on cyber security.[7]

1.3 Three basic security needs shape demand for different cyber security product types

Cyber security is no longer just firewalls and off-the-shelf virus software. In recent years, the breadth and depth of cyber security has evolved significantly. Today, it encompasses a sophisticated range of products and services that exist alongside a complex chain of activities used by organisations to build and operate their cyber security systems.[8]

These activities can be grouped into three fundamental security needs that shape demand for cyber security products and services. Combining the different security needs and product types, as shown in Exhibit 3, provides a helpful structure through which to understand the diversity of the global cyber security industry.

Exhibit 3:



Examples of product types and security needs

		Security need							
		1 Protection stack			2 Security operations			3 Underlying processes	
		Core system protection and management	Application protection	Protection of endpoints and data at rest	Security mgmt, assessments, and analytics	Incident recovery and response	Identity and access management	Governance, risk and compliance	Awareness, training, and oversight
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	▪ Assess current risk, maturity, and vulnerabilities and manage a full spectrum of security operations	▪ Respond to an incident by identifying, investigating & 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
Product types	Hardware	▪ Firewalls ▪ Next generation firewalls ▪ Router switch control ▪ Virtualised environment for malware detonation ▪ Sandbox	▪ n/a	▪ n/a	▪ n/a	▪ Intrusion detection system (IDS), as hardware	▪ 2FA hardware (e.g., tokens)	▪ 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	▪ 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
	Services	▪ Firewall configuration and management ▪ Threat intelligence and signature feeds ▪ Penetration testing ▪ Malware identification	▪ Application patch management ▪ Application testing/ code review ▪ SDLC	▪ Patch and configuration management – Endpoints/ Hardware – Network	▪ 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

SOURCE: Gartner, IDC, expert interviews, team analysis

Security needs

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

- **Building a protection 'stack':** The protection 'stack' is best understood as 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 that 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:** An organisation will only be successful in fending off cyber adversaries if it creates a strong culture of risk awareness. It needs clear rules for compliance, governance and risk-management. It also needs to ensure that all staff are well-trained and conscious of common cyber security threats.

The security needs of users vary across sectors and organisational sizes, and evolve over time depending on the maturity of their cyber security strategies, changes in technology and the shifting nature of cyber threats. For most organisations, these needs are met through a combination of their internal capabilities and by sourcing from external cyber security providers.

Product types

There are three main product types that are typically sourced to meet an organisation's cyber security needs: hardware, software and services. The markets for these different product types are generally distinct and display differing characteristics in terms of size and growth, exportability, job-creation potential and job quality (wage level and security of jobs). The three product types are also affected differently by major technological trends.

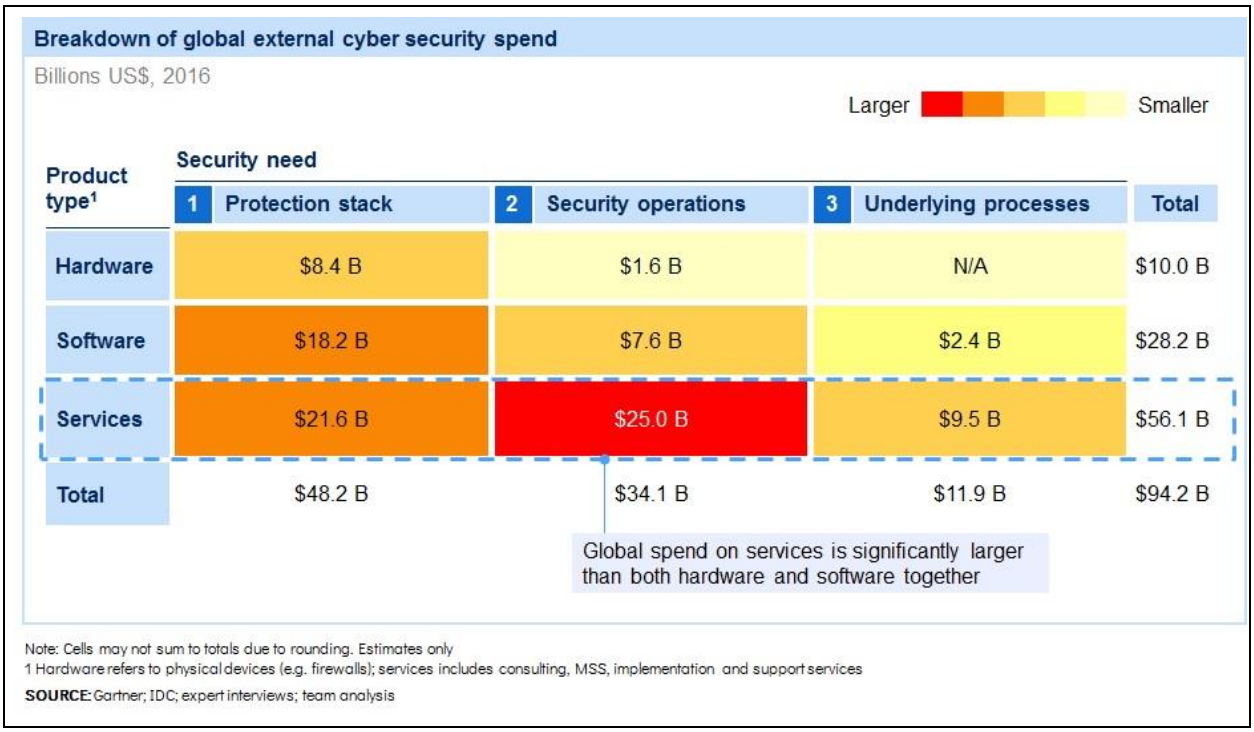
There are some areas of overlap between product types: for example, software is increasingly delivered as a service rather than a standalone product, and hardware devices are often combined with proprietary software. However, dividing the market into these three basic product types remains meaningful and useful for this analysis.

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 industry, accounting for 11 per cent of the industry's external revenue—equivalent to US$10 billion of worldwide cyber security spending. It is most heavily concentrated in the protection stack, with the bulk of revenue generated providing clients with core system protection and management. Outside the protection stack, Exhibit 4 shows that spending on hardware is very limited.

Exhibit 4:



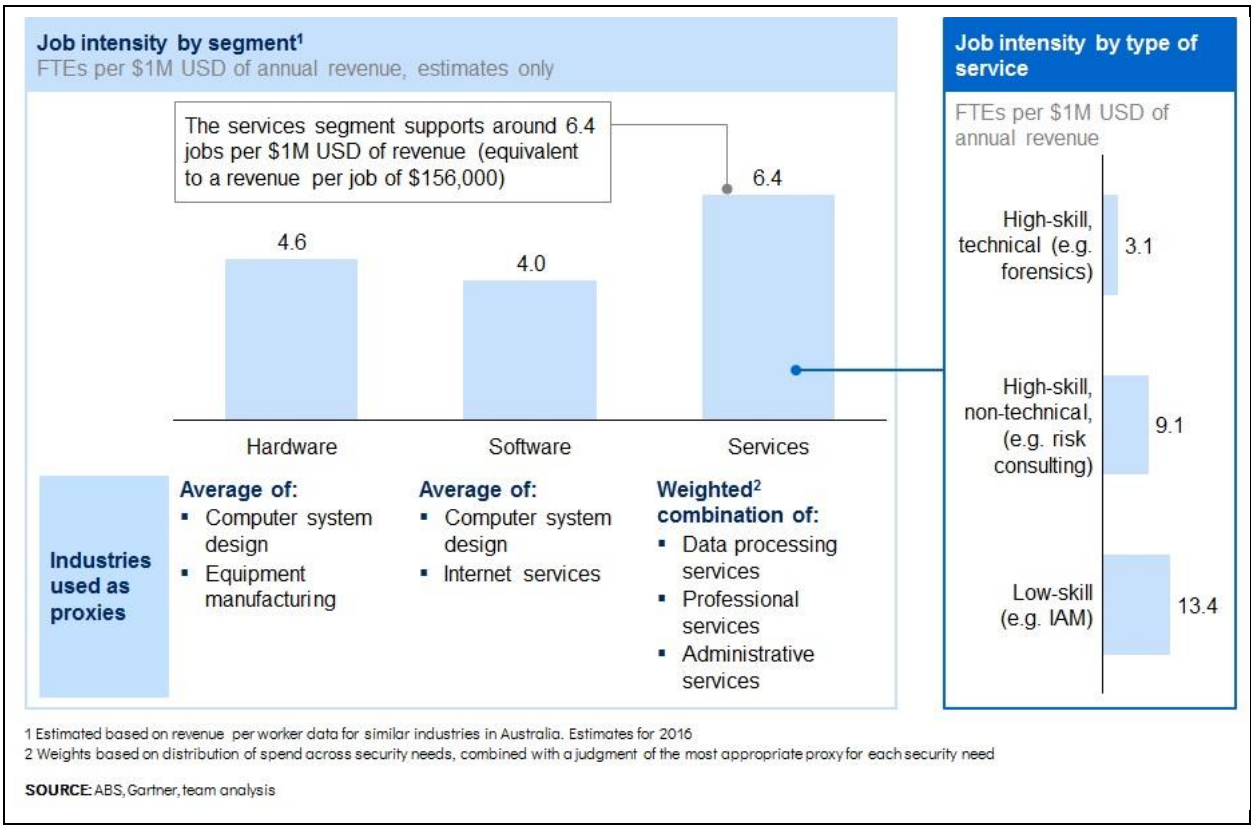
Growth: While the global demand for cyber security is projected to increase significantly over the next decade, hardware producers will receive a relatively small share of the industry's growth. The external global spending on physical IT protection equipment is estimated to increase by US$5.6 billion over the ten years to 2026, equivalent to an average growth rate of 4.5 per cent per year. This represents only a fraction of the projected total industry external demand growth of more than US$106 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 export of some cyber security hardware products with potential use in defence may be limited by the Wassenaar Arrangement, a multilateral export control regime comprised of 41 states including Australia.[9] It promotes

transparency and information exchange to ensure that the transfer of certain goods and technologies, particularly those with dual-use, does not enhance military capabilities that 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, representing a labour intensity that ranks between that of software and services, as seen in Exhibit 5. 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.

Exhibit 5:



Software

Software companies within the cyber security industry 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 industry's second-biggest product type. In 2016, it accounted for over US$28 billion of the world's total external cyber security spending, or 30 per cent of the industry's revenue, as shown in Exhibit 4. 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 decade to 2026, external demand for cyber security software is expected to increase at an average annual rate of 6.4 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: firms domiciled in the US control 61 per cent of the global market, while Israeli firms dominate around 18 per cent.[10] Country-specific rules protecting intellectual property could act as a barrier to export software, however.

Job creation and quality: Exhibit 5 shows that software tends to be less labour intensive than hardware or services, supporting an average of 4.0 full-time jobs per US$1 million of annual revenue. The quality of jobs in software is generally very high: the jobs are high-skilled and well paid, and there is low risk of automation impacting job security.

Services

Cyber security service providers meet a broad array of organisations' security needs. For example, they may help manage a company's core computer system defences, assess network vulnerabilities or provide a security strategy plan. Some act as 'first responders' when an organisation has suffered 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$56.1 billion, of the industry's global external revenue, as shown in Exhibit 4. Demand is highest in security operations, and specifically in security management, assessment and analytics. 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. Firms in this one segment attract more than a quarter, or US$15.6 billion, of the entire global spending on external cyber security services.[11]

Growth: Services enjoy the strongest growth outlook within the global industry. Over the next decade, the global spending on external cyber security services is expected to increase by 8.8 per cent per year. Growth is expected to be strongest for security operations, with an additional US$43.6 billion in demand forecast over the next decade.

Exportability: Cyber security services are exportable, but country-specific regulation and IT infrastructure can make services trade more challenging. For example, firms that help configure and manage a client's firewall may be limited in their reach by existing cross-border data regulations. Similarly, firms offering security management, assessment and analytics worldwide may require local offices to effectively service customers abroad. The assessment in Exhibit 6 shows that the exportability of incident recovery and response services is most limited by such factors, while application protection services and awareness, training and oversight are the least affected.

Exhibit 6:

Assessment of the 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: Subject to cross-border data regulations	Exportability: Need for in-country core technical team	Exportability: Need for in-country infrastructure	Overall exportability
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; team analysis

Job creation and quality: Exhibit 5 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 that of cyber security jobs in the hard- and software segment 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 previously done by people. This trend is particularly acute in the area of monitoring threats.

1.4 Technology is reshaping the industry

While every industry is affected by technological change, perhaps none is impacted more than the cyber security industry. 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 firms 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 general data flow of an organisation. 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 firms 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, whose multiplying endpoints and data types call for more sophisticated cyber defences. The vulnerability of these merged systems generates fresh demand for most security product types.

- **Mobile Internet:** The number of people owning a smartphone and using the internet continues to climb. A survey by U.S. research organisation Pew Research Center found that across eleven industrialized countries, a median of 68 per cent of adults owned a smartphone in 2015, with even higher rates of smartphone ownership in Australia (77 per cent) and South Korea (88 per cent).[12] Smartphones 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 smartphone 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.

- **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 as "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.[13] 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 firms increase their demand for applications to identify, analyse and manage cyber security threats. In the medium to long term, service providers will be disadvantaged but the transition to greater automation will likely increase the demand for services in the short term.

- **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 firms to save costs and simplify their IT infrastructure. The growing adoption of this technology has moved the potential area of malicious cyber activity from the corporate network to cloud computers managed by third parties. This is prompting firms to think differently about how to secure their operations. Several cloud computing providers are already offering an array of network protection products and services through the cloud itself. This reduces the need for firms to purchase their own cyber security infrastructure and dampens the outlook for hardware producers, while 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 a myriad of other devices of everyday use 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 patient'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, and generate new sources of opportunity for providers of cyber security solutions. This is likely to benefit software developers, as new types of endpoints need to be secured and threats identified.

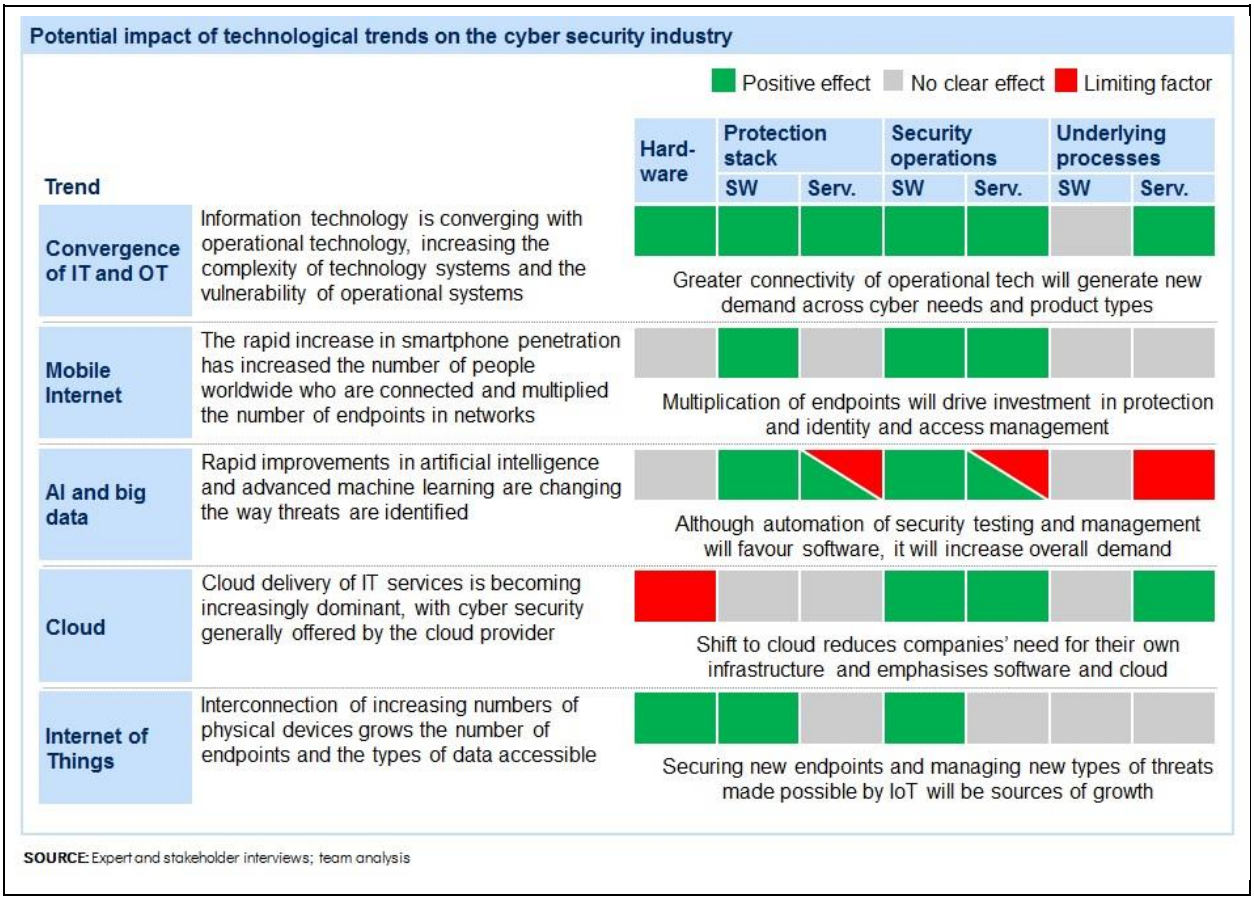
Exhibit 7 summarises how these five major technological trends may impact the cyber security industry and its products.

Several other important technologies could also have profound implications on the structure of the cyber security industry. Two that garner attention right now are blockchain and quantum computing.

Quantum computing is considered a breakthrough technology that is still in development but, if made a reality, would spark a major upheaval in the current cyber security industry. Australian researchers are currently 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 6).

Similarly, the disruptive power of blockchain technologies may bode well for Australia with its well-established financial services industry. It is difficult to predict how these trends will end up impacting different segments of the cyber security industry, but the potential for Australia to seize its competitive edge in both bitcoin and quantum computing is significant.

Exhibit 7:



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 ICT sector, cyber security evolves around the existence of an adversary: it has to constantly respond to highly unpredictable, destructive activities. Despite our best predictions and preparations, we never know where future attacks will come from and how the industry will be forced to reshape in response.

2. The potential of Australia's cyber security industry

2.1 Overview

Cyber security in Australia is a small but fast-growing industry. It is estimated to employ approximately 19,000 people, either as part of an organisation's internal cyber security workforce or through external cyber security providers, as shown in Exhibit 10. Total expenditure on cyber security amounts to approximately A$4.3 billion, equivalent to around five per cent of the entire Australian information technology sector.[14] Australian demand and employment is dominated by outsourced cyber security services, and more than three-quarters of this market is controlled by foreign firms—mostly operating from local bases and employing Australians. Software and hardware markets are also dominated by imports.

Despite this, there are already a number of Australian cyber security success stories. Australian cyber security providers have developed strong offerings in software and service niches. A number of our software firms have also joined global value chains and established a worldwide reputation for their products (see Boxes 1, 6, 8 and 9 for examples). Firms offering cyber security services, however, still lag behind their export potential. This is at odds with evidence that businesses in Australia generally earn much more revenue (relative to national GDP) from services than their peers elsewhere in the world, indicating that Australia has a fundamental country-specific advantage in services that cyber security firms have yet to use.

Given the small scale of our domestic market, Australia will struggle to become globally competitive in all segments of the cyber security industry. The Australian Government has selected priority sectors through the establishment of Industry Growth Centres; Australia should also concentrate its limited resources on parts of the cyber security industry that are both attractive and where Australia can compete most effectively. Analysis suggests that this includes software in areas of distinctive research capability, and services in the protection stack and in underlying processes. While these segments will be the initial focus of industry development, many of the actions of Government and ACSGN will also support the competitiveness of the industry as whole.

Australia should also consider the opportunity in cyber security to build on our 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 firms can develop distinctive, competitive offerings for global marketplace.

2.2 Local demand is strong, especially for services

In 2016, total external spending on cyber security by Australians and Australian organisations reached A$3.46 billion, and it is estimated that organisations spent a further A$919 million on their internal cyber security functions. To put that in context, Australia's external IT spending in 2016 was around A$85 billion.[15]

However, while external IT spending is forecast to grow by 2.8 per cent in 2017, Australian cyber security external spend is expected to grow by 7.5 per cent annually over the next decade. The growing risk awareness has led companies to invest more heavily in the safety of their networks and IT systems. According to a recent survey by the Australian Government's Computer Emergency Response Team (CERT Australia), 56 per cent of Australian companies increased their expenditure on cyber security in 2014. That's more than twice as many as in 2013, when 27 per cent said they had increased their investment.[16]

The demand for cyber security products and services in Australia is comparable to global demand trends, but with a larger emphasis on services. Exhibit 8 shows that 70 per cent of the local industry's external demand is for cyber security services, compared with around 60 per cent globally.

Exhibit 8:

Breakdown of Australian external cyber security spend

Millions A$, 2016

Larger — Smaller

Product type[1]	Security need: 1 Protection stack	2 Security operations	3 Underlying processes	Total
Hardware	$112 M	$20 M	N/A	$132 M
Software	$473 M	$282 M	$74 M	$830 M
Services	$1,030 M	$1,068 M	$399 M	$2,497 M
Total	$1,616 M	$1,370	$473 M	$3,459 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: Cells may not sum to totals due to rounding, estimates only
1 Hardware refers to physical devices (e.g. firewalls); services includes consulting, MSS, implementation and support services

SOURCE: Gartner; IDC; expert interviews; team analysis

Australian organisations, more than their global peers, rely on outsourced cyber security services. Almost three-quarters, around A$2.5 billion, of external Australian cyber security spending in 2016

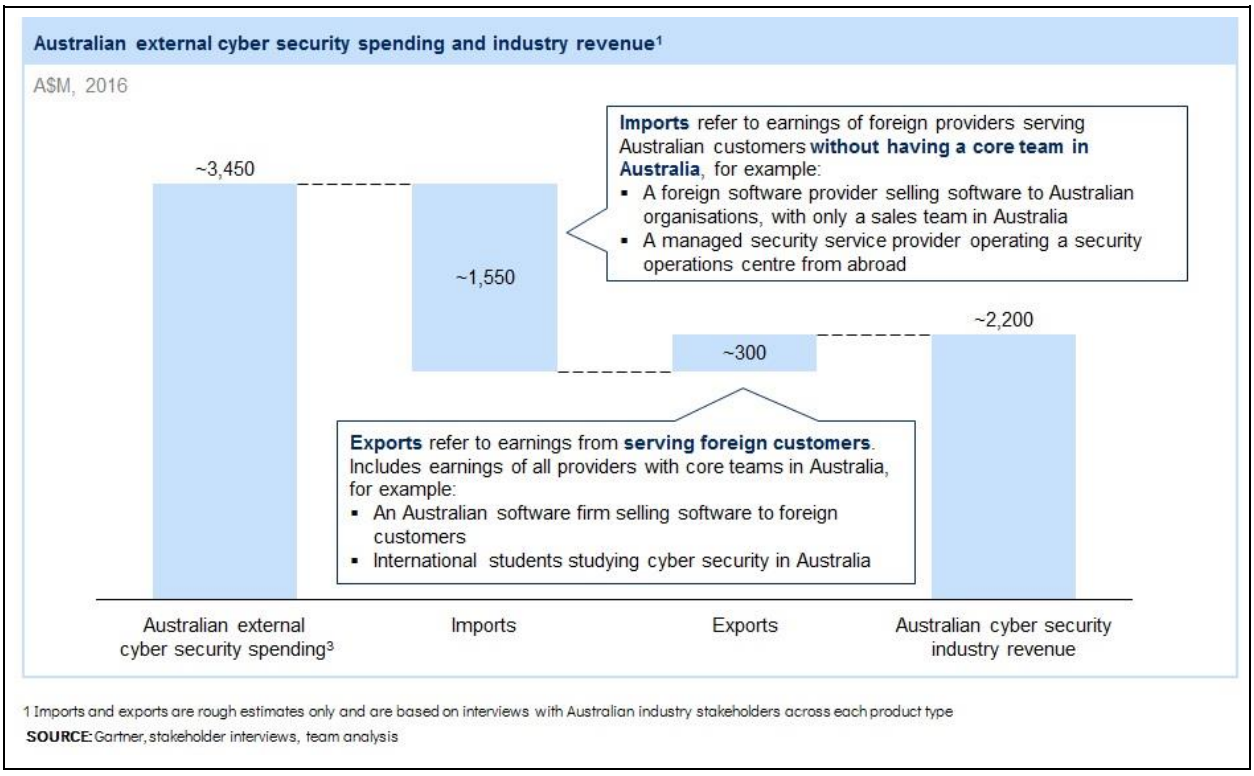
flowed into services. Exhibit 8 reveals that demand is particularly strong for services that strengthen the operational security of a business or other organisation. The dominance of the services segment in Australia may be partly explained by the particular structure of the local economy, where around 95 per cent of all Australian businesses comprise of small and medium-sized enterprises that 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.

2.3 Supply is dominated by imports

Much of the existing domestic demand for cyber security products and services is currently met by foreign providers. For example, there is currently not a single local firm among the 15 largest software providers by value in the Australian cyber security market. The combined market share of Australian firms is estimated to be less than five per cent. This is similar in hardware, with no major Australian hardware providers.

Exhibit 9:

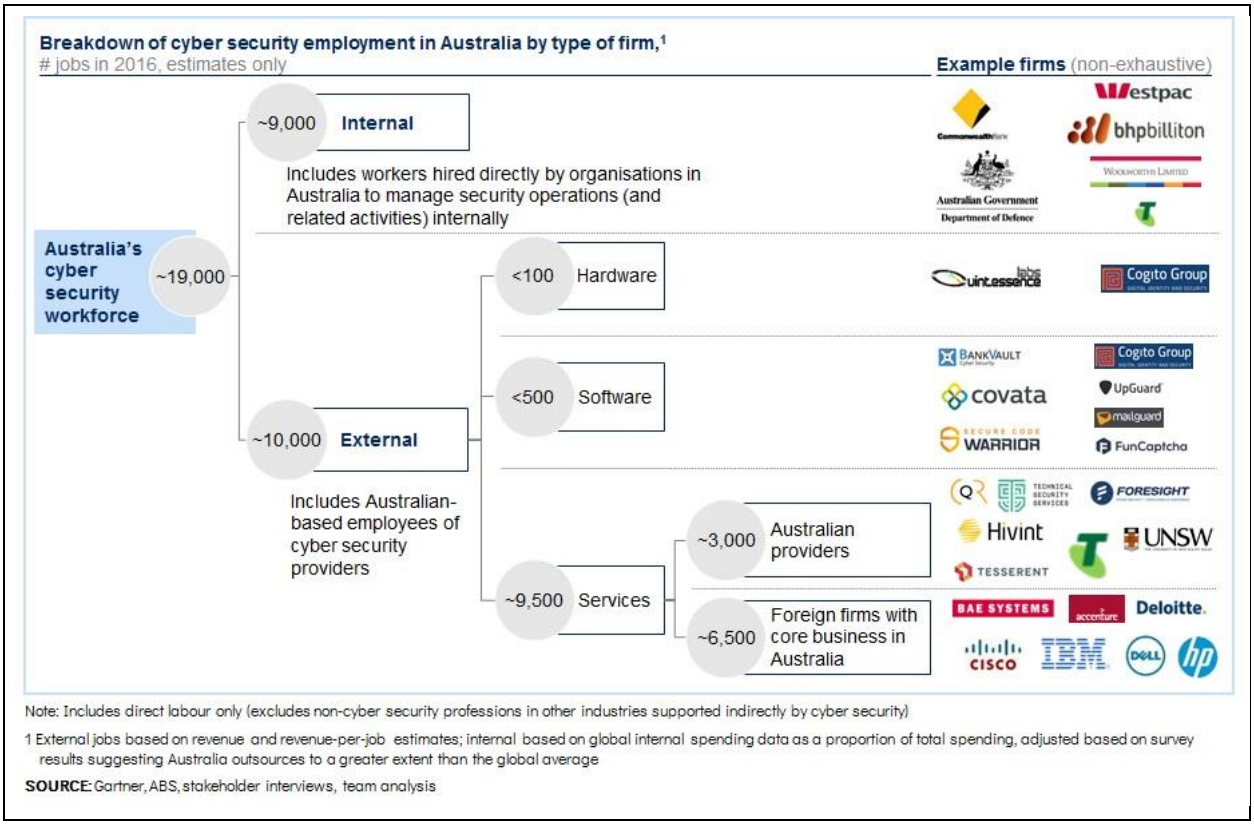


The representation of Australian firms is stronger in services—noting that the market data is not strong, interviews and other sources suggest that the market share of Australian home-grown services firms is about 25 per cent, while around half of the market is served by foreign-owned firms with core personnel in Australia (excludes foreign firms with only a sales presence in Australia).[17]

Putting these findings together provides a view of Australia's cyber security industry revenue—defined as the sales turnover of businesses employing cyber security professionals in Australia. Estimating industry revenue requires subtracting imports (defined in this context as cyber security products and services provided from abroad without having 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. Exhibit 9 shows that Australia's cyber security industry revenue is around A$2.2 billion.

The varying presence of different types of imports in each of the product types explains much of the current mix of employment in the Australian industry, which is shown in Exhibit 10. Hardware and software are typically directly imported to Australia and create very little permanent local employment. The total number of jobs in these two product types in Australia is probably less than 1,000.

Exhibit 10:



Note: Includes direct labour only (excludes non-cyber security professions in other industries supported indirectly by cyber security)

1 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

SOURCE: Gartner, ABS, stakeholder interviews, team analysis

There is a much greater presence of local cyber security providers in services. Paired with the generally higher labour intensity of services, it is estimated that local cyber security services firms

are supporting around 3,000 jobs in Australia. Still, foreign service providers with local operations remain the largest employer in Australia's market for external cyber security. These multinational corporations currently employ almost 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 firms make a very significant contribution to the overall workforce—only exceeded by employment of in-house cyber security teams, which is estimated to be around 9,000 workers.

2.4 Australian firms have existing strengths in software and services

There are areas of both software and services where Australian firms have been successful in both domestic and international markets. In software, there is a strong 'beachhead' of Australian firms in the area of security operations.

Box 1: Making Sense of the Data EXPLOSION

The world is amassing data like never before. But how much of it do we really use? Vast amounts of the growing stockpile of information that's crowding server centres across the globe has long lost its immediate business value. Such "dark data", as it is commonly known, comprises a jumble of information that time has rendered irrelevant: expired customer files, records of previous employees, old emails, notes and presentations, historic financial statements or outdated accounts.

Hoarding masses of obsolete data poses a security risk, however, especially if they contain sensitive information. Many organisations have thus begun to tidy up their electronic storage rooms to avert cyber criminals, and Australian IT firm Nuix is among the most powerful to help them master this task.

Nuix is one of Australia's leading cyber security firms. Founded in 2000 by a team of computer scientists, it has developed a powerful forensic software to collect, process and analyse huge amounts of digital data. Its ability to sift through terabytes of large and complex files at high speed has made it a go-to address for leading organisations around the world who need fast and accurate answers—including the United Nations, the U.S. Secret Service, Interpol and the Department of Defence.

Nuix's software helps clean up unknown, messy and risky data that's hidden in dark corners of corporate networks. It helps detect and respond to cybercrime, manage insider threats and find rapid evidence in a law suit or audit. Most recently, a global group of investigative journalists used Nuix's optical-character recognition technology to review 11.5 million documents leaked from a Panama-based law firm.

The investigation, in which Nuix's electronic discovery software was able to digest 2.6 terabytes of data in just 1.5 days, unveiled a web of hidden offshore accounts entangling several country leaders and other high-profile public personalities. Today, Nuix remains headquartered in Sydney, with additional offices in the U.S., England, Ireland and Germany.

Firms such as Covata, StratoKey, Airlock Digital and Huntsman Security have developed successful software products and established market presence both in Australia and international markets. Nuix, an Australian data analytics and security firm, was the platform chosen by the International Consortium of Investigative Journalists to analyse the files in the Panama Papers (see Box 1).

Box 2: game changing high-grade encryption for the field

Penten is a new cyber security company, located in Canberra ACT, that is revolutionising the use of deployable high grade encryption technologies for mobile solutions. Penten also specialises in cyber deception methods and operational integration of cyber security strategies.

Increasingly users need access to data from remote locations and when data is mobile, it has more utility. To address this need, Penten has developed the AltoCrypt™ family of solutions to allow mobile access to highly sensitive information from anywhere, without compromising security.

The AltoCrypt™ *Stik* is an 'all in one' deployable high grade encryption device that gives organisations operating senstive and classified networks an easy to carry and simple to use secure access solution. AltoCrypt™ *Stik* supports mobility both inside and out of the workplace by replacing a large briefcase based system with a small USB-sized stick. AltoCrypt™ *Stik* is small, lightweight, powered by USB, operates anywhere and is low cost. AltoCrypt™ *Stik* delivers a very low network and physical signature.

AltoCrypt™ *Stik* is designed, manufactured and assembled across Australia and the United Kingdom through partnerships with other Australian based companies.

The founders of Penten are experienced cyber security entrepreneurs, who have already successfully developed and sold an award winning cyber security firm to a major US defence contractor. With a track record of scientific invention, commercialisation and export success of cyber security technology from Australia, the Penten team is now focused on innovating in secure mobility and the emerging field of cyber deception.

Partnerships and collaboration are key to their success. AltoCrypt™ solutions were developed in partnership with the UK cyber security firm Amiosec Ltd. Penten have now also partnered with Downer Group, a leading Australian provider of engineering services, to improve the cyber resilience of critical infrastructure providers.

Australian cyber security software firms are also exporting their products in the protection stack security need (e.g. Mailguard) and in underlying processes (e.g. Secure Code Warrior). The representation of local firms in hardware is weaker, though the innovative work of penten (see Box 2) and QuintessenceLabs (see Box 6) demonstrates that Australian firms can still play in niche areas of hardware.

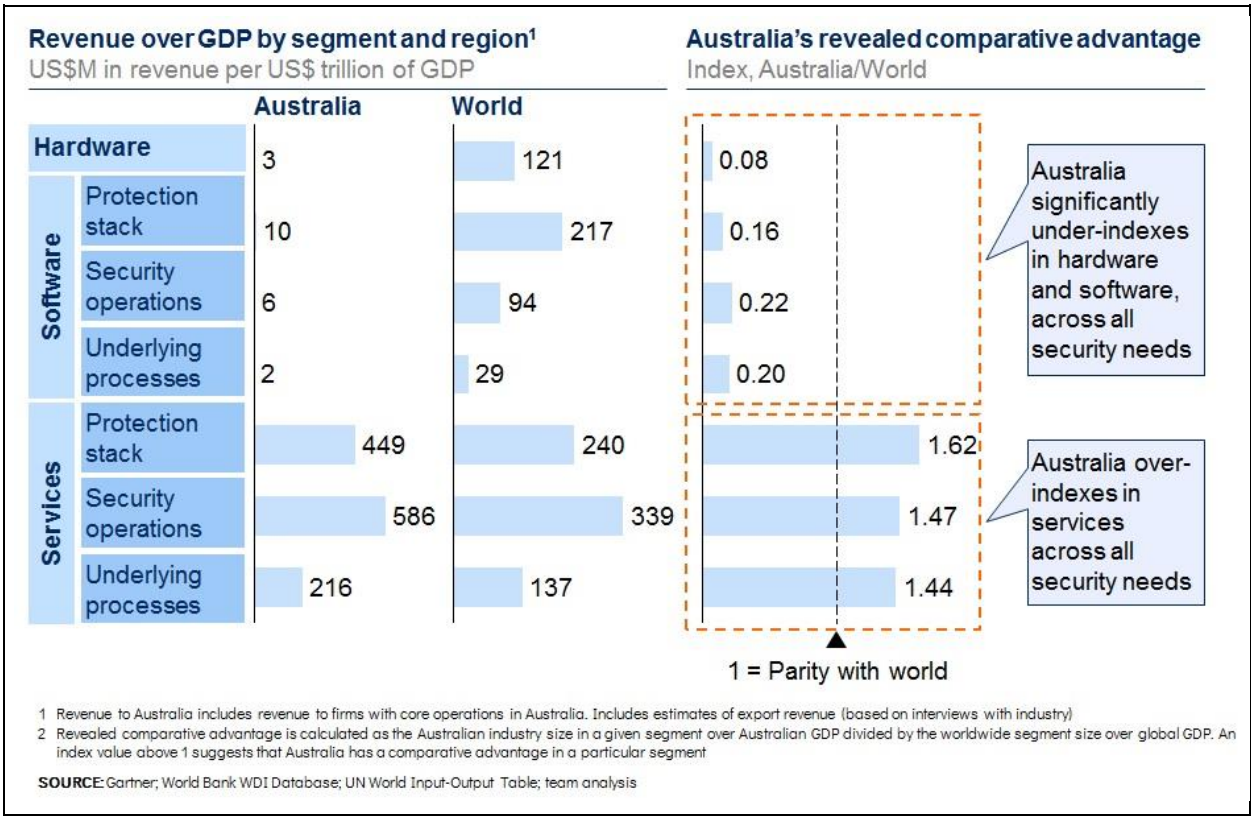
The services segment in Australia contains a large number of local firms. In the protection stack, Australian firms such as archTIS and Shearwater Solutions provide services in security architecture and penetration testing. Security operations, while dominated by the large multinational managed services providers, includes some smaller Australian firms and Telstra. It is in the third security need, underlying processes, that Australian firms are strongest, with a range local providers active such as Hivint, Cogito Group and Enosys. In addition, Australia's universities are increasingly active in the training aspect of underlying processes, offering a range of cyber security courses (see Box 11 for details).

Yet, very few of these firms are currently exporting their services. Among those that do have a significant presence abroad is Bugcrowd. The company was founded in Australia in 2012, but has since shifted its headquarters to San Francisco, partly to get better access to venture capital. Telecommunications company Telstra has ventured into South-East Asia, through a partnership with Telkom Indonesia comprising a jointly managed data network and security services. Other examples for cyber service providers with large international operations include risk-analysis firm UpGuard and endpoint-protection firm 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.

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. How much more or less successful than the world average is a country when supplying a particular good or service? The RCA index tries to answer that question: values above 1 signal that a country enjoys a comparative advantage in the supply of a certain product or service. In contrast, index values below 1 indicate a disadvantage relative to other suppliers globally.

The analysis in Exhibit 11 reveals that Australian firms and foreign firms with core operations in Australia already earn a much higher revenue (relative to national GDP) in services than their average peers worldwide, highlighting a substantial comparative advantage in the services segment of the cyber security industry. The situation, however, is reversed in the hardware and software segments of the market, where the current revenues (relative to national GDP) of Australian firms and foreign firms with core operations in Australia are significantly lower than the equivalent world average, signalling a comparative disadvantage.

Exhibit 11:



2.5 Australia's opportunity: focus initially on a limited number of segments

Australian cyber security firms have proven that they can be successful abroad, even in highly competitive markets such as the US and Europe. To emulate the success of these local 'pioneer' firms across the wider Australian cyber security industry will require Australia to identify and focus on its country-specific competitive advantages. It also requires developing the talent base and resources to turn its strengths into a competitive edge. While the role of ACSGN is to promote and improve the competitiveness of the entire industry, it will also work to support the development of a number of initial focus segments.

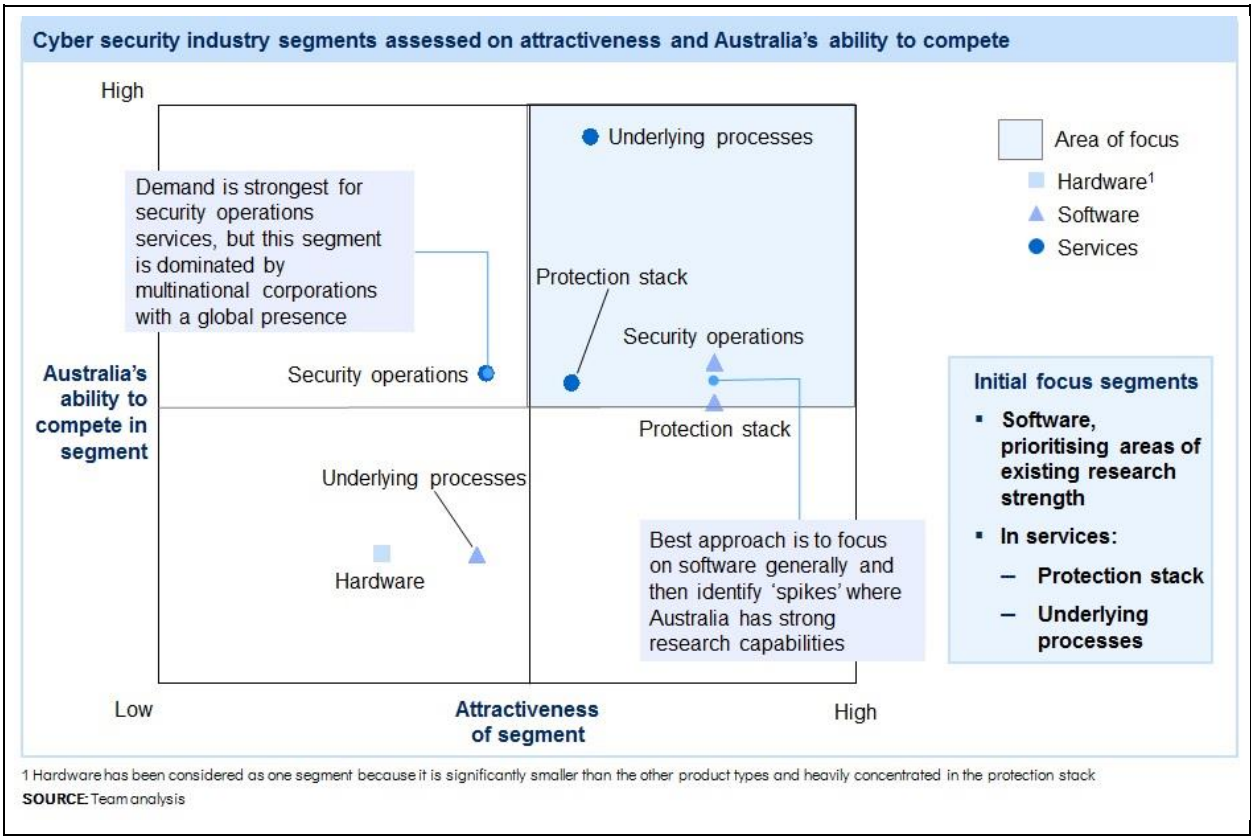
A rigorous framework of analysis has been used to identify several segments within the Australian cyber security industry that promise to generate the largest opportunities for the Australian economy over the next decade. Seven segments appear most noteworthy: three types of software and three types of services meeting the 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 and competitiveness.

- **Attractiveness:** 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.

- **Australia's ability to compete:** Based on Australia's existing presence, any revealed comparative advantage, and the segment's match with Australia's skill profile.

As a result of this analysis and extensive interviews with industry participants, which are shown in Exhibit 12, three focus segments stand out: software, services in the protection stack, and services in underlying processes.

Exhibit 12:



1 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: Team analysis

Software

Software is an attractive segment in both security operations and the protection stack, with strong existing size in the protection stack and the largest increase in demand forecast for security operations. Software products are highly exportable, and generate high-quality jobs. Software will also be positively impacted by the convergence of IT and OT, mobile internet and the Internet of Things, that will multiply 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 software segments, the best approach for Australia is to consider software as one broad segment and then identify specific areas of research capability upon which we can build 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), but these will need to be further refined through more detailed assessment of our comparative research strengths.

Though attractive, there is not as strong evidence for Australia's ability to compete effectively in software. Our current revenue in software is very low, which implies a lack of comparative advantage. However, there are several firms that have succeeded both domestically and in export markets. These include Nuix, which has become internationally renowned for its forensic capabilities (see Box 1), Huntsman Security and Stratokey. These beachhead firms 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 prevent attackers from gaining access to organisations' networks, and protect applications and endpoints (see Box 3 for 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 is currently the second largest segment in the Australian industry—after security operations services—and is forecast to experience continued strong demand growth.

While harder to export than software, protection stack is still relatively exportable due to less need for in-country technical teams to provide the services than in security operations. It requires a strong supply of medium- to high-skill workers, which matches well with the skill profile of the Australia cyber security workforce. The convergence of IT and operational technology (OT), and the Internet of Things are two trends that lead to a higher number of network endpoints and a stronger need to protect these endpoints. While automation may have some negative impact on employment in this segment, strong demand growth will mean that the productivity shock from automation should be limited.

Australia already has a strong domestic protection stack services segment, with the highest revealed comparative advantage among all seven segments. In interviews with CISOs and CIOs, services such as penetration testing and network security architecture are regularly identified as the industry's current 'spikes'. Australian firms have also been successful in exporting in this space: Mailguard, for example, has developed an email and cloud security service that is now sold in 27 countries worldwide. Their solution builds on a platform of “Software as a Service” (SaaS) to create what is effectively a niche-managed service providing email filtering.

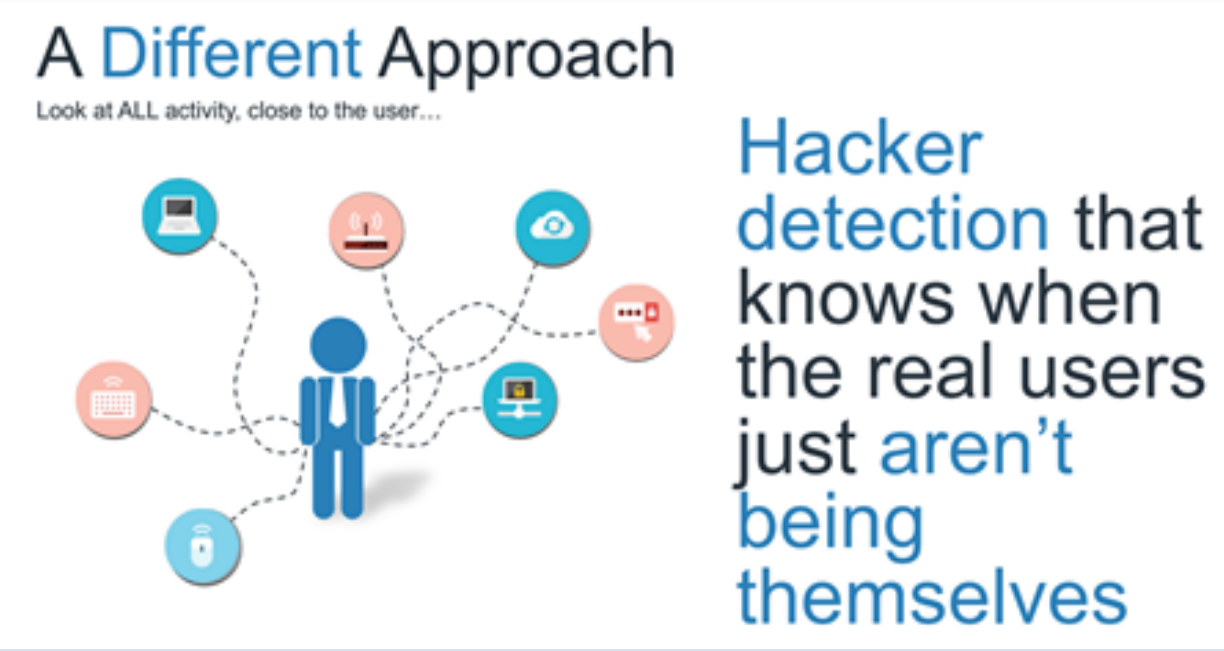
Box 3: Securing endpoints through behavioural analytics

ResponSight is an Australian data science company that uses anonymous behavioural analytics to provide an innovative approach to detecting malicious cyber actors and security breaches.

While traditional systems actively search for threats, ResponSight's solution focuses on monitoring endpoints in fine detail for unusual activity by gathering analytics and taking snapshots to determine the fingerprint of each endpoint. Using its cloud-based analytics engines, ResponSight consolidates and analyses millions of activities to understand what is normal online behaviour for every legitimate user. When behaviour differs, an alarm is raised indicating a user's endpoint could have been compromised, malware is present or the device is being used by a different (authorised/unauthorised) user.

ResponSight collects numerical, mathematical and statistical data about how the endpoint is used and can be distinguished from other user and entity behavioural analytics (UEBA) technologies that mostly gather their behaviour data from log data or centralised Security Incident and Event Management (SIEM) repositories. This means that other UEBA data is rarely complete and often out of sequence. By working on the endpoint, ResponSight is as close to the actual user as possible, providing a detailed fingerprint. This technology can be integrated with other existing enterprise technologies.

ResponSight's philosophy is simple - to deliver reliable technology and service to help customers address security risks by reducing the time it takes to detect a breach across organisations that have multiple user devices. Founded in 2015, ResponSight has plans to expand its customer base into the US later in 2017. The founder of ResponSight has over 20 years experience in security and sees the organisation's growth being driven by its ability to deliver on its promises and making a difference in a complex aspect of cyber security.



Services – underlying processes

Services are the dominant product type in addressing the security need of underlying processes. Specific services delivered here include the development of cyber security strategies, risk and compliance policies, employee training, and measures to raise the general awareness of cyber security risks within organisations (see Box 4 as one example). While underlying processes in services is the smallest of the services segments in Australia and globally, it still accounts for more than 10 per cent of Australian external demand.

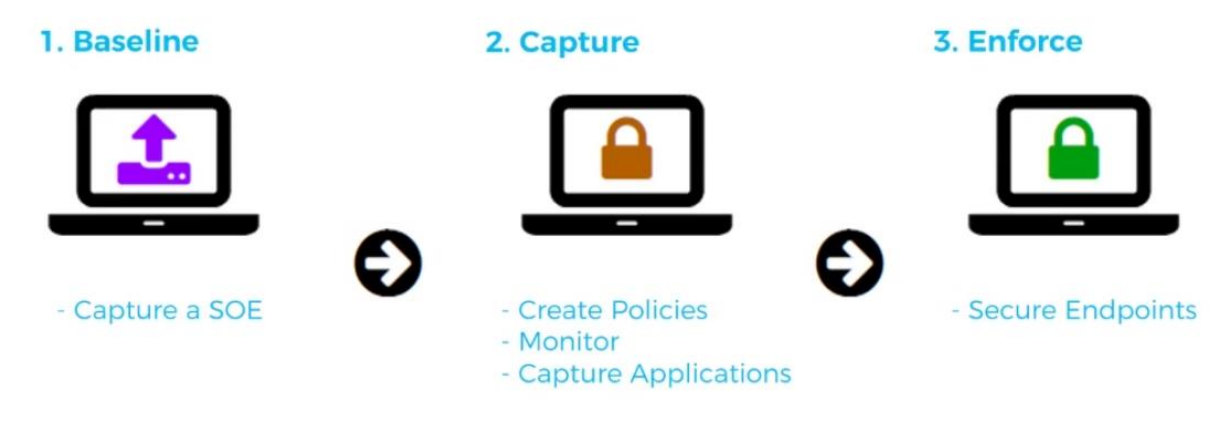
Box 4: keeping cyber intruders at bay

Australian firm Airlock Digital, founded in 2013, helps keep cyber intruders out of an organisation's network by creating so-called application whitelists. Application whitelisting involves specifying which applications (e.g. programs, software libraries, scripts and installers) are permitted and can be executed on a computer system. The goal of whitelisting is to protect computers and networks from potentially harmful applications. The Australian Signals Directorate considers the method to be one of the most effective to mitigate targeted cyber intrusions.

But what sounds simple in theory, can be challenging to put into practice for small and large organisations alike. That's where Airlock tries to make a difference. It offers application-whitelisting solutions that it says are cheaper, less complex and require less resources to perform successfully.

Unlike signature-based file blocking (blacklisting) such as antivirus software, Airlock's solution proactively sets up barriers to ensure attackers cannot execute malicious and unknown code on an organisation's networks. Each Airlock deployment results in a unique whitelist according to customer needs. Airlock then verifies, monitors and records all file executions across the organisation, permitting only authorised files to load. This makes Airlock extremely effective at preventing both opportunistic and sophisticated attacks, including ransomware and other targeted attacks, allowing the customer to react faster to cyber threats.

Airlock Digital's solution has proven effective in many industries. Key clients include government agencies, large enterprises and small firms in Australia. More recently, Airlock has also started growing its international customer base.



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 'exported' through international student enrolments.

Education-related travel services are already Australia's largest services export, accounting for around six per cent of our total exports in 2015.[18] Their quality is highly regarded abroad, particularly in the Asia-Pacific region. As continued strong global growth in cyber security creates demand for skilled professionals (see the next chapter for details on skills shortages), our experience in export of education means that Australia'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. However, the total number of international students in Australian cyber security courses—estimated to be around 200—are still very low.

Similarly, Australia already has a strong ecosystem of local firms 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.

****

These three segments will be the initial focus of efforts to develop a globally competitive Australian cyber security industry. However, many of the strategies and actions proposed to be undertaken by ACSGN and others in support of these segments will also benefit the wider industry. The set of focus segments will also be regularly reviewed by ACSGN to respond to changes in the industry structure and technology trends that have not been anticipated.

2.6 Playing to our industry 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 that 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 that they require.

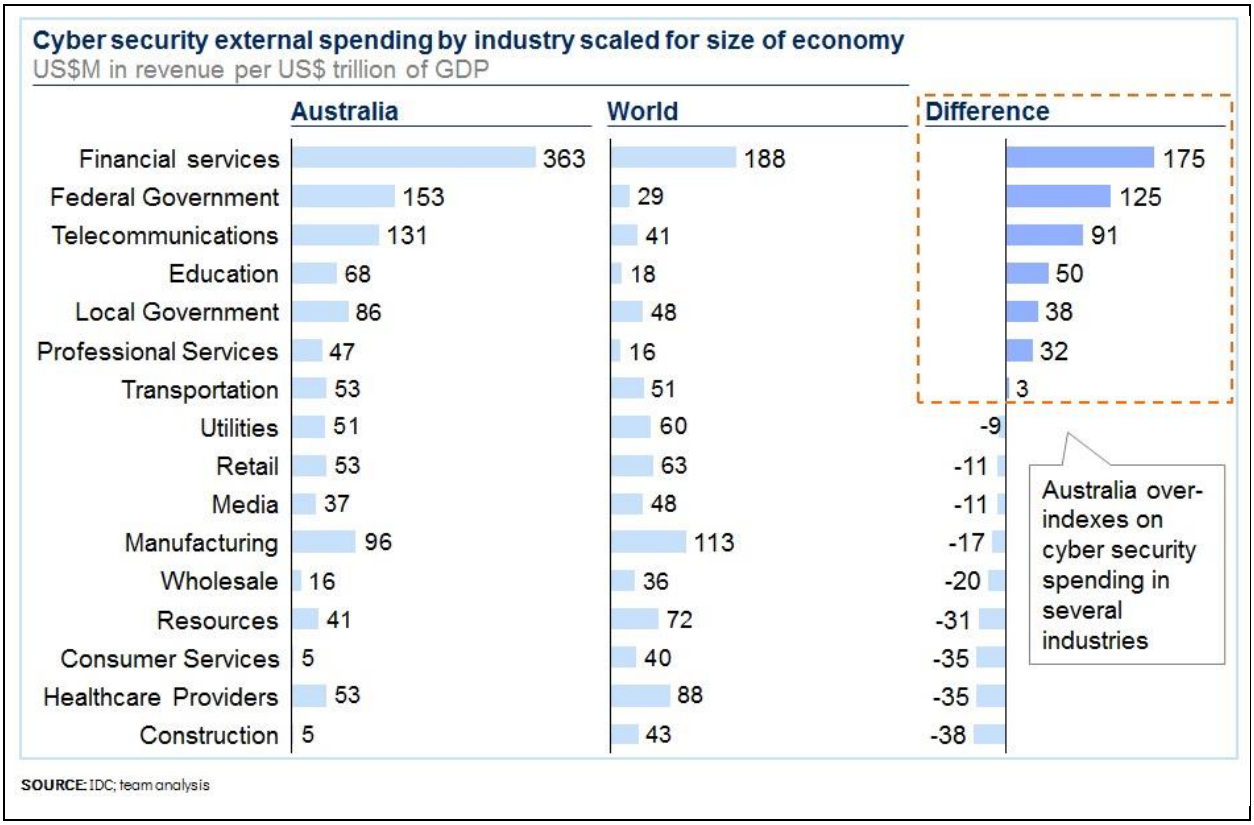
Therefore, there are potential sources of comparative advantage for Australian firms in the industry composition of our cyber security demand, the industry mix of the broader economy, and in our export performance. Two examples of such industry strengths are financial services and resources.

Financial services

Australia financial service firms are the largest users of cyber security products and services 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 firms are elsewhere in the world, as illustrated in Exhibit 13. 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 firms 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 firms. This would allow them to quickly build scale and reach international markets. Interviews with successful Australian cyber security firms indicate that a number have pursued this strategy effectively. The fintech incubator Stone & Chalk has also recently partnered with Data61 and industry to host a series of events on the opportunity for Australia to lead in cyber security for fintech, and is planning to launch a Fintech Cyber Innovation Lab.[19]

Exhibit 13:



Resources

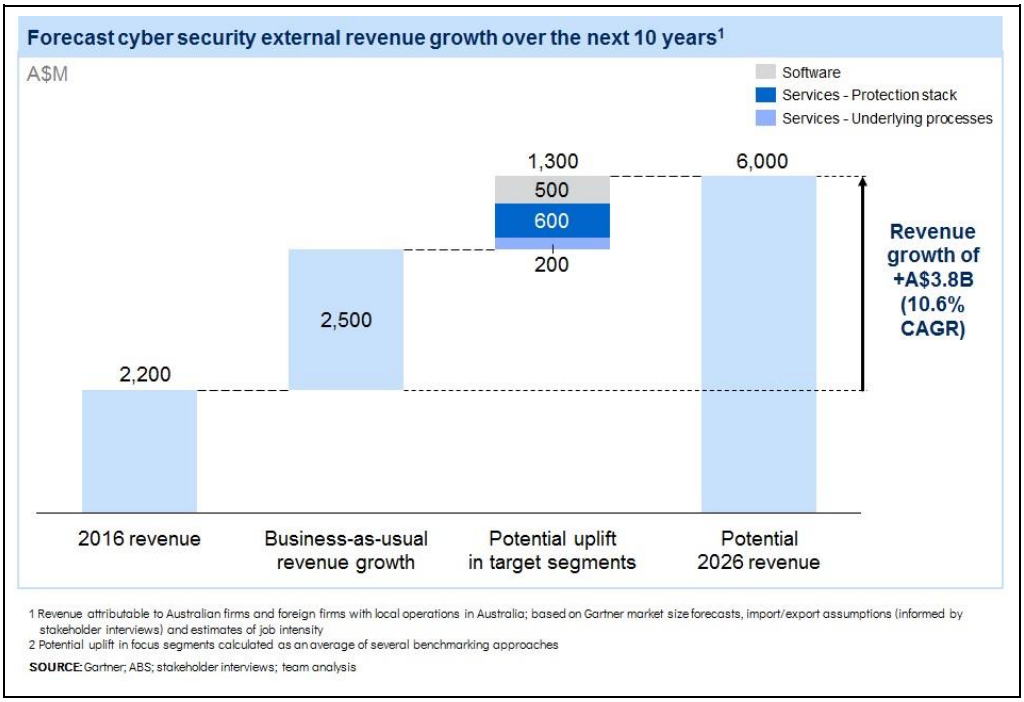
Resources have been a major engine of the Australian economy, especially in the last decade. Natural resource rents were almost five per cent of Australia's GDP in 2015, while globally they accounted for just 1.7 per cent.[20] Resources also dominate our exports to the rest of the world: even at the end of the mining boom, in 2015, commodities made up six of the ten most valuable Australian goods or services exports.[21] Being a resources powerhouse has allowed Australia to produce some of the world's largest mining companies and to develop world-leading mining technology.

The convergence of operational technology and IT creates new security issues for the mining industry—and provides a significant business opportunity for Australian cyber security providers in the focus segments. Exhibit 13 shows that the cyber security demand from resources firms in Australia (measured as spending relative to GDP) is currently lower than the cyber security investments of resources firms globally. However, this could change quickly, as the Mining Equipment, Technology and Services sector in Australia remains strong and is still home to several major global resources players. Improvements in software will be particularly valuable for resources organisations who need to manage the risks from the integration of their operational technology into the broader network infrastructure.

2.7 The size of the prize: benefits for Australia

The potential benefits to Australia from developing a globally competitive cyber security industry are substantial, even when compared to the existing strong forecast growth in the industry over the next decade.

Exhibit 14:

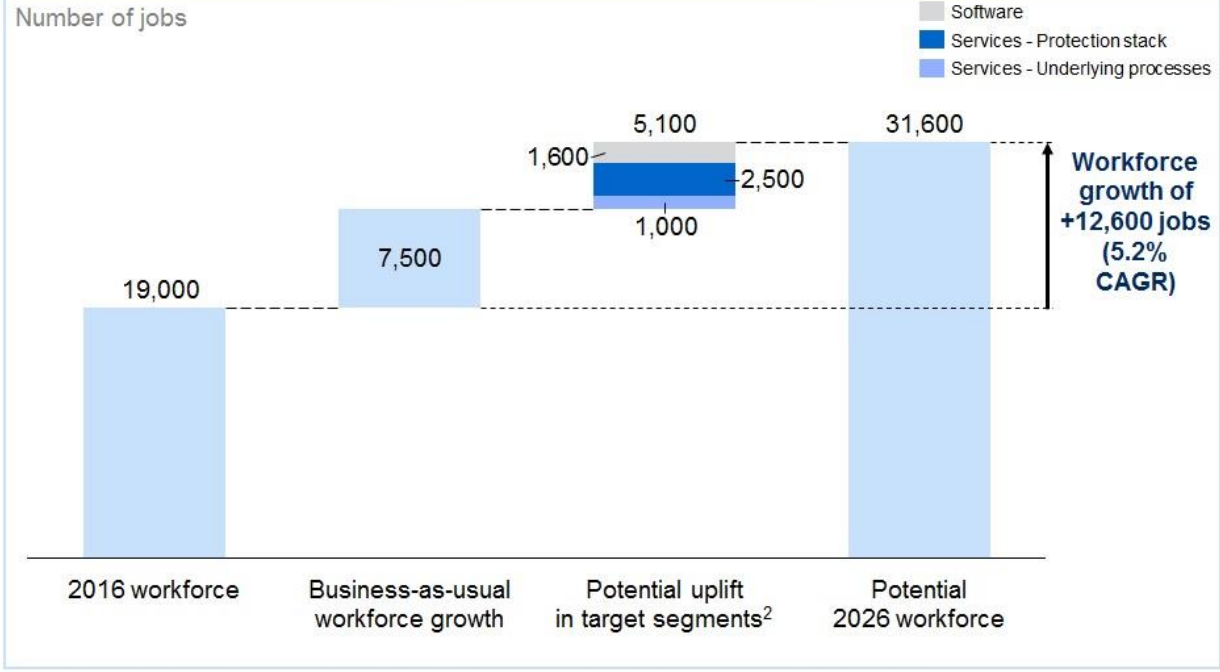


Those 'business-as-usual' forecasts imply that industry revenue will more than double in the period 2016-26 from A$2.2 billion to A$4.7 billion, as shown in Exhibit 14. If Australia undertakes concerted actions focused on supporting the growth of three initial focus segments, it is estimated that industry revenue in 2026 could increase to A$6.0 billion, which equates to an annual growth rate of almost 11 per cent over the decade.

This uplift in revenue would generate new jobs and a significant increase in the size of the cyber security workforce. 'Business-as-usual-growth' forecasts, illustrated in Exhibit 15, suggest that that employment in cyber security in Australia will increase from around 19,000 to more than 26,000 by 2026. Actions to promote the development of the focus segments could add a further 5,100 jobs to the cyber security workforce, Exhibit 15 shows. Given estimates of natural retirement and net loss to overseas jobs, this implies that Australia will need more than 16,000 additional workers to enable the industry to meet its growth potential.

There will also be significant spillover benefits to the wider economy. Having a stronger cyber security industry will enhance Australia's global reputation as a trusted and secure business environment. This could increase demand for other Australian goods and services exports. A growing local market for security solutions will also lower the cost related to data breaches and malicious cyber activity for Australian organisations.

Exhibit 15:



1 Based on Gartner market size forecasts, import/export assumptions (informed by stakeholder interviews) and estimates of job intensity
2 Potential uplift in focus segments calculated as an average of several benchmarking approaches

SOURCE: Gartner, ABS, stakeholder interviews, team analysis

These benefits will complement positive outcomes from measures already announced in Australia's Cyber Security Strategy. For example, the Australian Government said in the Strategy that it will sponsor research to better understand the cost of malicious cyber activity to the Australian economy. This research will also help identify the specific financial gains that come with a more effective domestic cyber security industry.

3. Challenges to Australia's cyber security industry

3.1 Overview

Three major challenges are currently detracting from the growth outlook for Australia's cyber security industry: a lack of focus in research and commercialisation; market barriers that hinder smaller local cyber security providers from becoming scalable, export-oriented firms; and a shortage of job-ready workers. This chapter provides an overview on these challenges, while Chapter 4 (*Building a competitive Australian industry*) lists a range of recommended actions to address these obstacles to growth.

The first challenge is related to Australia's current research, development and commercialisation system. To be sure, R&D is important for many industries. In cyber security, however, where customer success is driven predominantly by a firm's ability to offer effective technology, a failure to invest in R&D can be fatal. Australia's cyber security industry can only thrive and produce innovative, cutting-edge technology if there is strong support for research and commercialisation.

This chapter shows that Australia's public investment in cyber security R&D lags that of global industry leaders, such as the US and Israel. A breakdown of grant data suggests that Australia's national funding for cyber security research currently lacks strategic focus. Interviews with industry participants reveal that research collaborations between universities and businesses—viewed as crucial for a vibrant, innovation-driven industry—are mostly limited to larger firms, and often fail to meet expectations of both parties. Funding data also indicate that it is more difficult for Australian cyber security startups than for their global peers to access early-stage venture capital for the commercialisation of innovative products.

There are strong signs that Australia could make better use of the existing array of funding sources and Chapter 4.1 (*Grow an Australian cyber security ecosystem*) offers some solutions, including coordinating our research efforts on a limited number of topics that match our existing capabilities and support the focus segments.

The second challenge lies in overcoming market barriers that hamper local firms in their efforts to scale their operations and become leading exporters. Many startups lack a clear understanding of the specific needs of their customers. Many also lack the trust and credibility to win an anchor customer for their products and services. Complex procurement processes in both government and the private sector become an additional hurdle: they prevent many smaller and younger firms from scoring a large customer contract. Chapter 4.2 (*Export Australia's cyber security to the world*) outlines a range of strategies to tackle these issues, such as relaxing current procurement procedures.

Thirdly, Australia has difficulty attracting and retaining cyber security talents. While the skills shortage is affecting the cyber security industry globally, there are signs that the lack of cyber talent

in Australia is among the worst in the world. Australian firms struggle to find job-ready cyber security workers despite offering high wage premiums. This chapter reveals that Australia will likely need around 11,000 additional cyber security workers over the next decade—for technical as well as non-technical positions—just to meet the industry's 'business-as-usual' demand forecasts.

There are signs that the formal education system fails to produce enough job-ready cyber security graduates in Australia. However, employers themselves may also be hindering the supply of skilled workers, with limited opportunities for cyber security graduates to gain work experience. Many companies have also failed to develop strong training pathways that could prepare workers from outside the industry, who bring a similar skills profile, for jobs in cyber security.

There are ways to address these bottlenecks of skills supply, however, and Chapter 4.3 (*Make Australia the leading centre for cyber security education*) outlines the most promising ones. For example, partnerships between training institutions and industry can help scale existing cyber security courses and improve the job-readiness of graduates.

3.2 Research and commercialisation

Cyber security firms 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 and revolutions in technology challenge security providers to constantly stay ahead of the curve by developing innovative products. While Australia has strong capabilities in cyber security research, lack of nationally coordinated themes and poor collaboration undermine the commercialisation of that research into marketable software. Inadequate incentives for commercialisation also weaken Australia's ability to lead on innovation 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. Cog Systems is one Australian cyber security company demonstrating both these elements in its solutions (see Box 5).

Australian providers can also compete on scope, such as having a more comprehensive offering than others and allowing cyber security users to acquire a wider array of products and services from one vendor. An analysis of the attributes that matter most to cyber security customers when choosing a vendor gives valuable insight into what makes a cyber security firm competitive.

Box 5: integrated technology from world leading cyber security R&D

The Internet of Things (IoT) is exposing users, original equipment manufacturers (OEMs) and platform operators to new risks. Cog Systems has developed technology that enables the commercial market to benefit from government grade security for connected devices for the first time, through a commercially available off-the-shelf solution. The Cog Systems solution protects connected devices from current and future threats by responding to threats from the broader security landscape and to specific requirements from devices' OEMs.

Cog Systems leverages their D4 Secure Platform™ to assemble a software development kit (SDKs) for specific categories of connected devices. D4 Secure SDKs™ protect organizations and their users with embedded virtualization technology that integrates easily into the users' device. This embedded virtualization enables the user to continue to access their data securely and without restriction to run any application. No longer will your VPN run in the same security domain as third-party downloaded apps.

Built on Australian developed technology, such as the L4 Microkernel heritage and design principles, the D4 Secure Platform™ leverages the inherent benefits of virtualization to drive towards the concepts of modularity with the fundamentals of security, trustworthiness, robustness, fault tolerance, and adaptability.

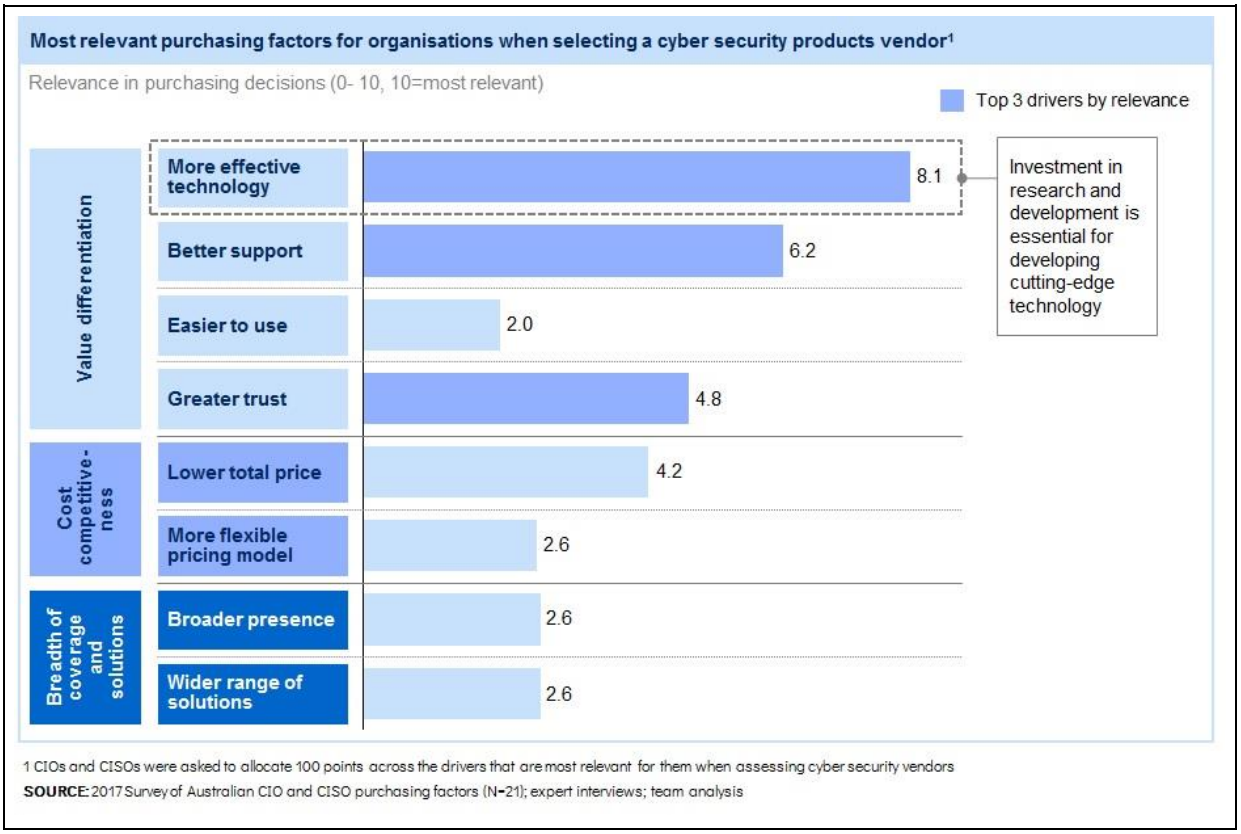
The initial reference product, the HTC One A9, secured by D4™, is an ultra-secure smartphone built on a type 1 hypervisor with enhanced storage encryption, non-bypassable VPN, support for nested VPNs, plus many other advanced security features that play an increasingly important role in the security process.

D4 Secure products provide for an intuitive security solution for OEM integration and in-channel and end-user enablement – the best of all worlds in mobile security.

Together, the founders of Cog Systems have over 40 years' experience across the design and implementation stages of mobile and IoT devices. Motivated to ensure all individuals receive the highest level of mobile security, their goal is to ensure all mobile and IoT devices are secure. Cog Systems customer base in Australia and internationally includes government and enterprise across a variety of regulated and non-regulated industries.

A survey among leading Australian Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) reveals that the customer appeal of cyber security firms hinges to a great extent on technological leadership. 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.[22]

Exhibit 16:



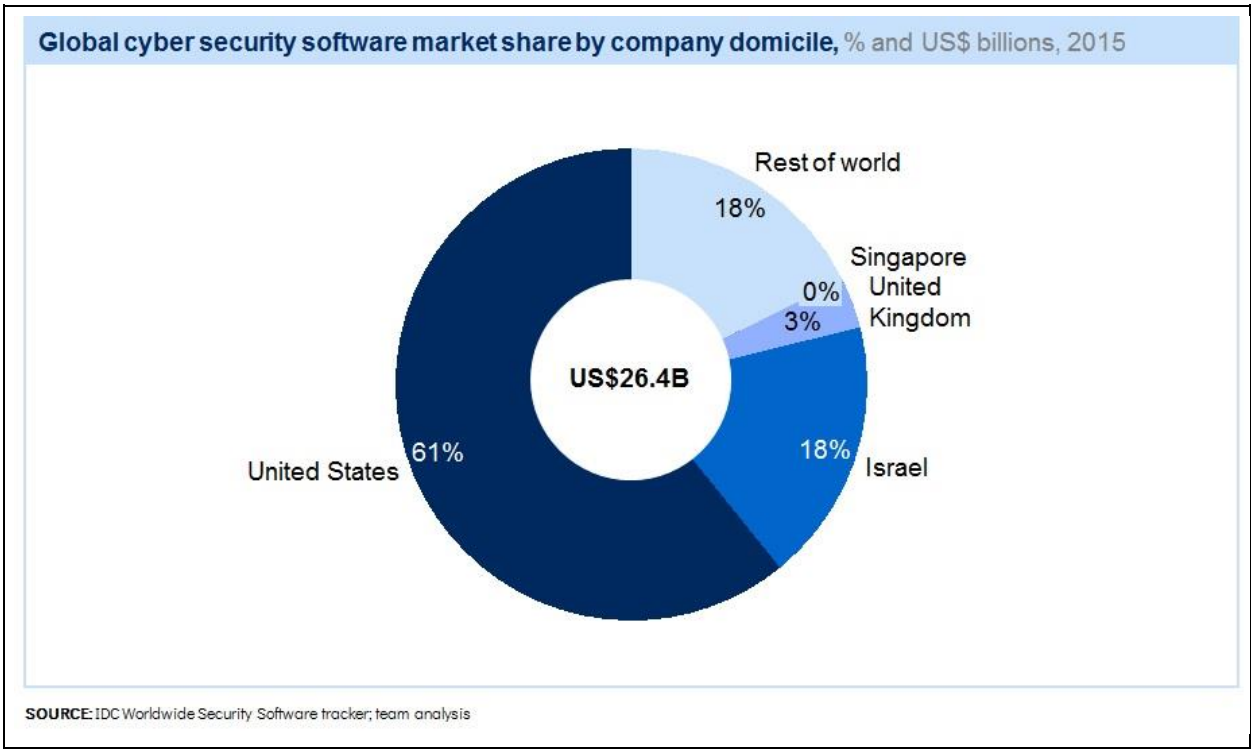
However, developing the most effective technologies is resource intensive, and requires firms and research institutions to invest heavily in R&D to unearth new ideas and collaborate for their commercialisation. Governments can support these efforts in several ways, either directly through research grants 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. They can also fund programs to improve research collaboration between universities and industry.

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 heavily invest in R&D. For example, the market power of American cyber security software firms—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 Exhibit 17—coincides with a significant commitment to R&D.

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

American firms 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.

Exhibit 17:



Israel, traditionally boasting some of the highest defence spending in the world, also provides strong government support for cyber security R&D. Israeli firms 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. Israeli firms spent around US$200 million on cyber security R&D in 2014, according to figures from Israel's National Cyber Bureau obtained by Israeli newspaper Haaretz.[23]

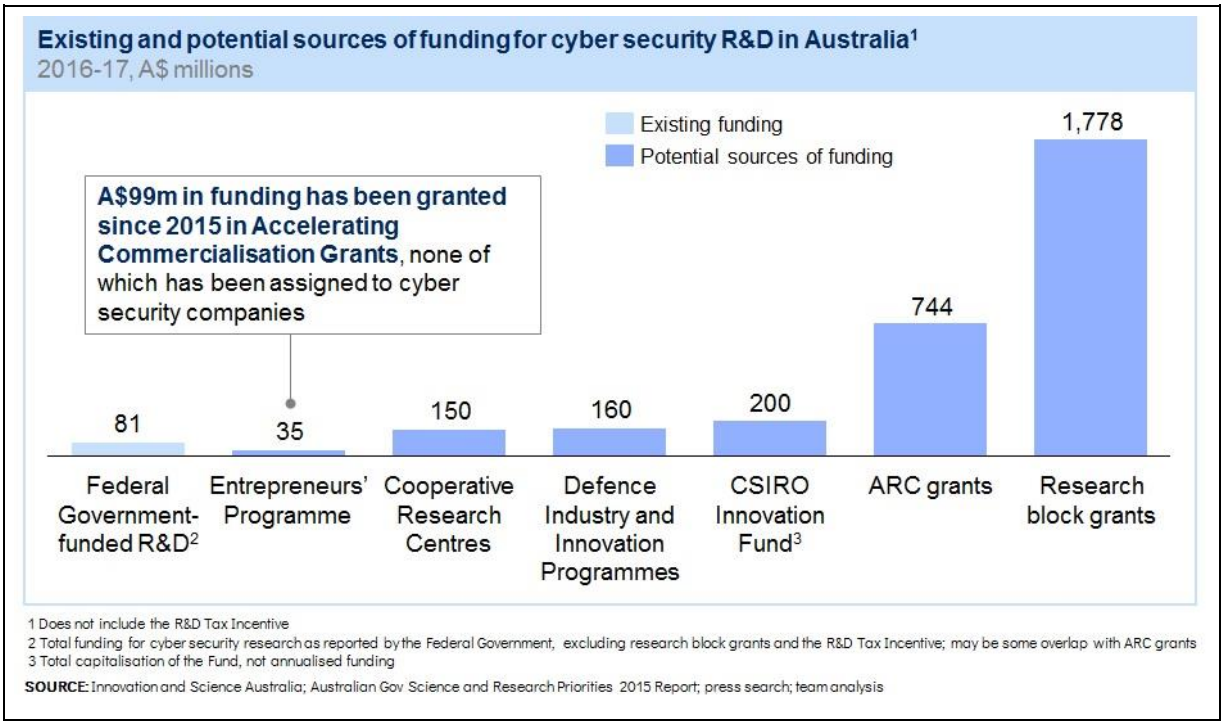
Several other countries have begun to play catch-up in recent years, but their R&D budgets for cyber security still appear modest compared to those of the US or Israel. For example:

- The United Kingdom government has pledged to create a new 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 latest National Security Strategy, which will inject the equivalent of US$2.37 billion (GB£1.9 billion) into the British cyber security industry over the five years through 2021. Some of the money will fund "cyber start-ups and academics to help them commercialise cutting-edge research and attract investment from the private sector".[24]
- The Singaporean government recently announced a five-year plan to build new R&D expertise and improve its cyber security capabilities. The 2013-2020 National Cybersecurity R&D Programme invests around US$20 million per year (or 27 million Singaporean dollars, equivalent to S$190 million over seven years) in cyber security research and innovation.[25]
- The Australian Government has made cyber security a national priority for science and research. Its current expenditure on cyber security R&D, as shown in Exhibit 18, 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.[26]

Australia could better use public funding sources for cyber security research

There are signs that Australia could increase the firepower of its public spending on cyber security R&D simply by making better use of existing funding channels. A breakdown of available grant schemes, as shown in Exhibit 18, indicates that several potential sources to finance cyber security research remain largely untapped.

Exhibit 18:



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. However, due to difficulties in the collection of block grant data it is unclear to what extent these funding tools are currently used to finance cyber security R&D. It is fair to assume that Australia still has scope to increase the use of university block grants for cyber security R&D funding.

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.[27] Access to ARC funding will be improved from 2017 as cyber security is listed as an Industrial Transformation Priority under the Industrial Transformation Research Program (ITRP). This program provides funding for both postgraduate training centres and research hubs.

Accelerating Commercialisation is an area of focus across Australian governments with the aim of helping small and medium-sized businesses to commercialise novel products, processes and services. Around 180 firms have received financial assistance over the past two years through a competitive grants process with a total value of A$99 million.[28] Cyber security firms have not received any assistance from this programme over that period, which may be resulting from a lack of quality applications.

Cyber security researchers may also be able to make better use of the CSIRO Innovation Fund, a joint government-private sector initiative that invests in start-up, 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.

The Department of Defence is another major source of R&D funding in Australia. In the fiscal year ending June 2017, it paid industry, academia and research organisations an estimated A$160 million to assist them with the development of new, innovative technologies for military use.[29]

The Department will play an even bigger role as a potential funding source for cyber security research in the future. This year, it plans to launch a new fund, dubbed the Next Generation Technologies Fund, that aims at fostering emerging technologies in the earliest stages of development. One of the nine priority areas for the fund is cyber. The fund will invest A$730 million (over the decade to June 2026) in strategic next-generation technologies that have the potential to deliver game-changing capabilities to Defence. The annual funding will increase over the decade.

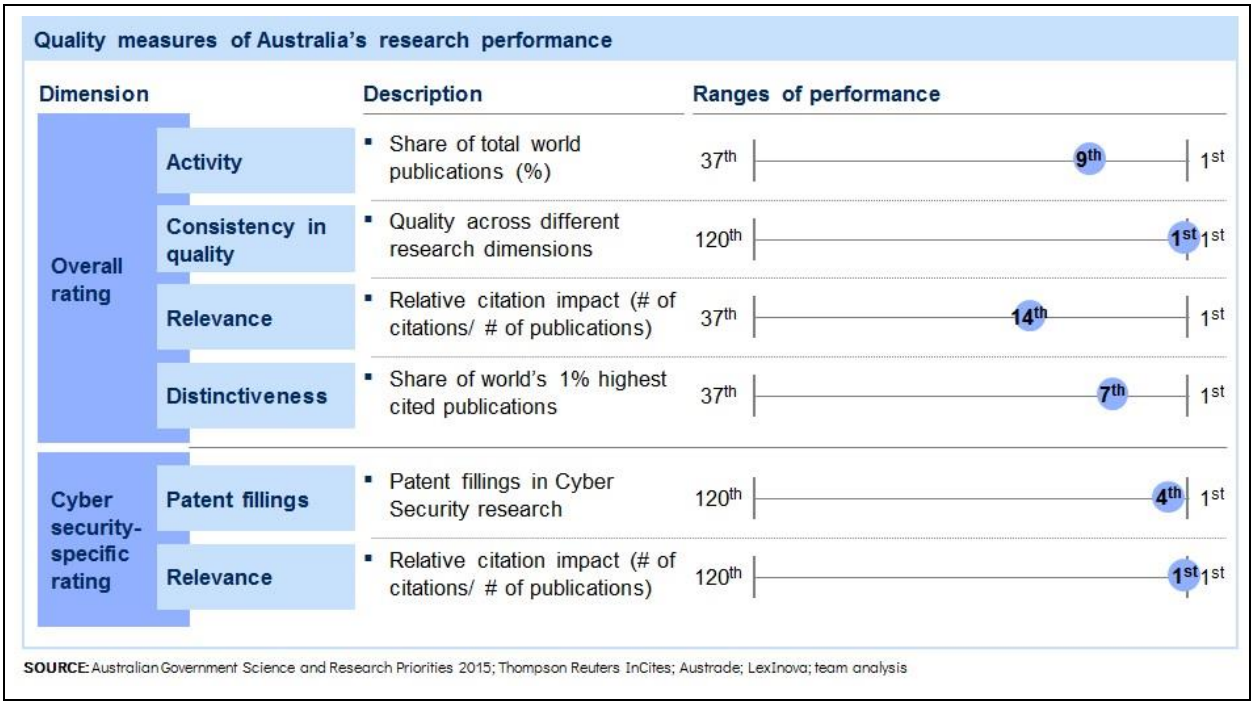
Lastly, there is potential to encourage more R&D in cyber security through the Australian Cooperative Research Centres (CRC) Programme, which supports industry-led research collaborations with around A$150 million per year. These centres are designed to improve the competitiveness, productivity and sustainability of Australian industries, especially where Australia has a competitive

strength. CRCs are established through merit-based selection rounds; and at present, there is no CRC established with a focus on cyber security.

Australia has world-class research, but there are blockages throughout the innovation system

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.[30] Cyber security research from Australia ranks highly in global comparison, Exhibit 19 reveals.

Exhibit 19:



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.[31] Australian universities thus appear well placed to lead the knowledge creation and spearhead the invention of new technologies in cyber security.

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 (ANU) and the University of New South Wales (UNSW) are already considered on the leading edge of research into quantum computing and its potential applications for the cyber security industry (see Box 6).

Box 6: Australia's lead in the global quantum race

It's 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, whose existence was long thought to be a distant vision.

Rapid technological advances by IBM, Google and others have stoked fears, however, that quantum computers may become a reality much sooner than many people think. The National Security Agency in the US last year warned that the time to act and build "quantum-resistant cryptography" is now.[32] The Canada-based Global Risk Institute puts the odds of a quantum computer cracking key security algorithms by 2031 at 50 per cent.[33]

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: 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.[34]

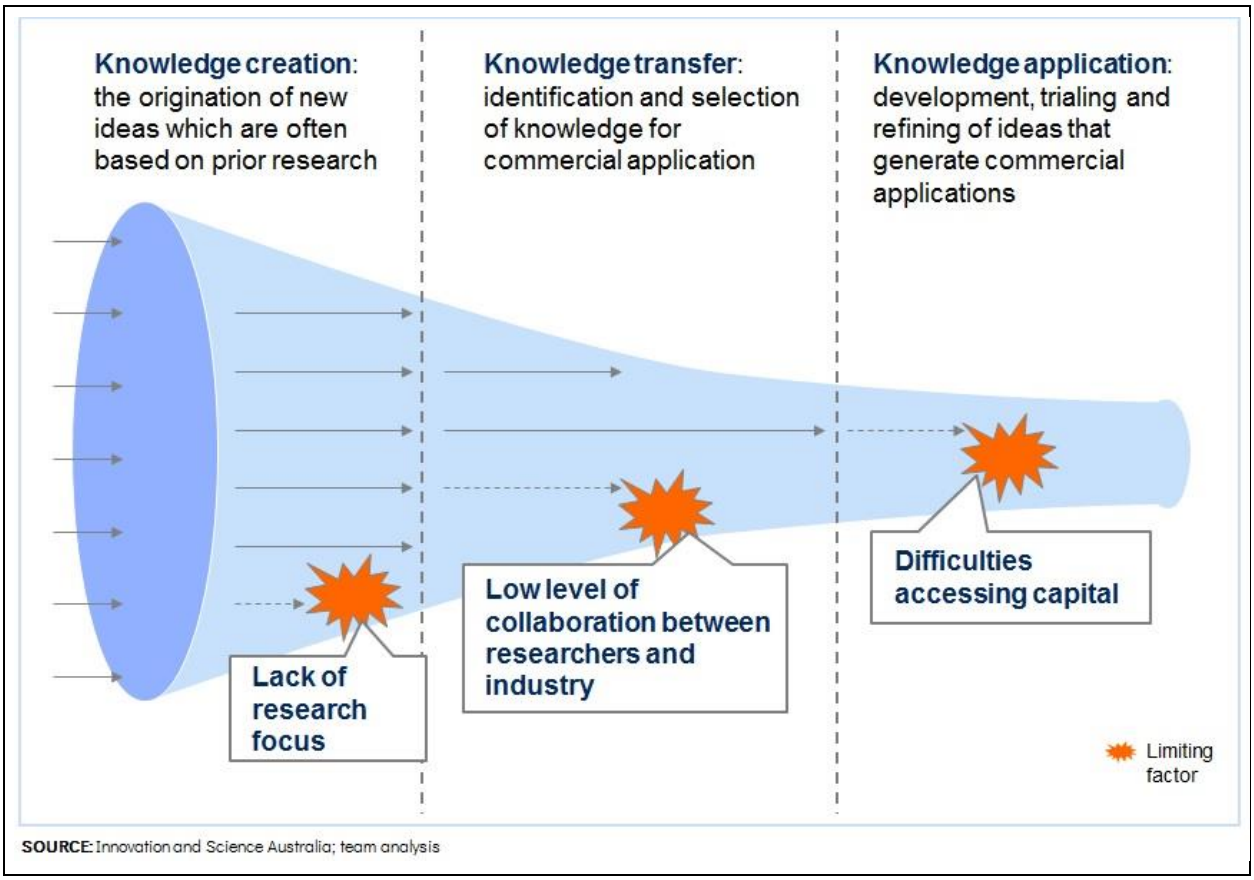
While scientists around the globe are exploring a range of exotic materials—from synthetic crystals to dye pigments—to build a quantum computer, Australia's research group is on track to develop the world's first quantum computer in silicon. "Our Australian centre's unique approach using silicon has given us a two to three-year lead over the rest of the world," said Professor Michelle Simmons, director of the Australian Research Council Centre of Excellence for Quantum Computation and Communication Technology, or CQC2T.[35] "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 Commonwealth Bank, the CQC2T's work is crucial for Australia's nascent cyber security industry.[36]

Startups such as QuintessenceLabs have already begun to seize the 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 invented and commercialised a so-called 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 machine, no bigger than a mobile phone, can generate these truly random codes by splitting a laser beam in two at very high speed and converting the resulting signal to numbers.

QLabs, formed in 2008 as a spin-off out of The Australian National University in Canberra, has received numerous accolades. Its clients include IBM and major Australian lender Westpac Banking Corp, which recently bought a 16 per cent stake in the firm and is utilising QLab's encryption capabilities to boost the security of its banking business.[37] Headquartered in Canberra, QLabs also runs a research lab at a NASA facility in Silicon Valley and was named 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.

An often-cited criticism, underpinned by OECD data, is that Australia struggles to translate its academic strengths into marketable solutions.[38] The cyber security industry is no different, as illustrated in Exhibit 20. Several obstacles are blocking the innovation pipeline in cyber security and hamper the commercialisation of high-quality research ideas.

Exhibit 20:

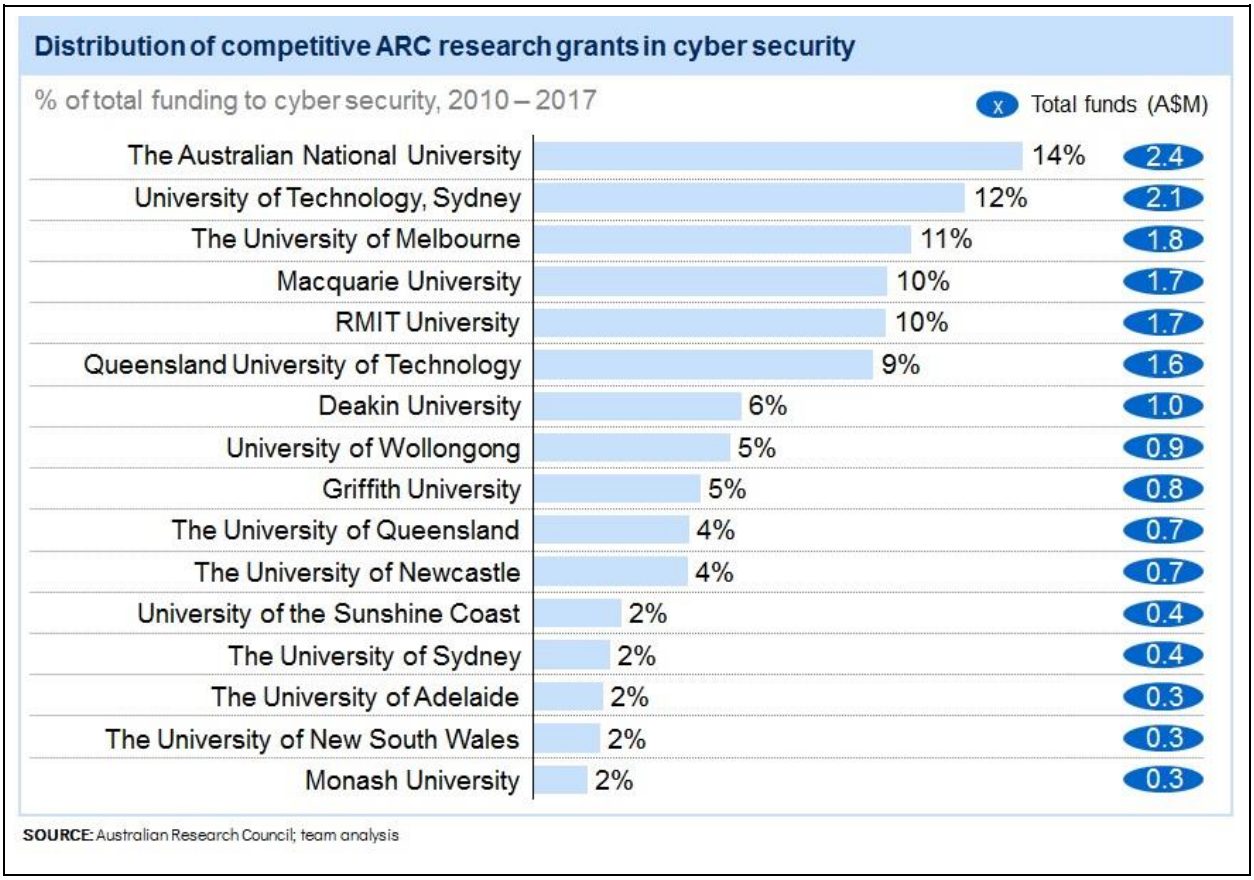


SOURCE: Innovation and Science Australia; team analysis

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 Exhibit 21, 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.

Exhibit 21:



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.[39] 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. Chapter 4.1 (*Grow an Australian cyber security ecosystem*) identifies a number of actions to help improve the focus of Australia's cyber security research

Collaboration between industry and research is weak

A vivid exchange between academia and industry is necessary to help researchers validate the practical applicability of their research and to ensure research ideas get translated into practical applications. University scientists who cultivate a close collaboration with companies will 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.[40] Yet OECD data show that the ties between academia and industry in Australia are the weakest in the developed world: only three 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.[41]

The situation is more ambiguous in the Australian cyber security industry. Some of the largest companies in the country's information-technology sector are acutely aware of the benefits of partnerships with local universities. For example, Commonwealth Bank of Australia is investing A$15 million to support researchers at UNSW who are striving to build the world's first silicon-based quantum computer in Sydney (see Box 6).[42]

The investment comes on top of government funding worth A$26 million for the Centre for Quantum Computation and Communication Technology, based at UNSW. An additional A$10 million of research funding for the project comes from Telstra, the nation's biggest telecom, which has assigned its team of data scientists to work directly with UNSW 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.[43] Quantum computing has potentially profound implications for cyber security, particularly through cryptography.

Macquarie University and telecommunications firm Optus partnered in 2016 to establish a multi-disciplinary cyber security hub with a joint investment of A$10 million. While primarily set up to ease the industry's skills shortage, the "Optus Macquarie University Cyber Security Hub" also offers consultancy services and undertakes research in a variety of areas, including security risk analysis, trustworthy computing and cyber governance (see Box 11).[44]

Meanwhile, US technology company Cisco Systems has been instrumental in developing the Security Research Institute at Edith Cowan University in Western Australia.[45] The company is also a founding member of the Australian Cyber Security Research Institute (ACSRI), which describes itself as the country's first coordinated strategic research and education effort between national cyber security agencies, industry and researchers.[46] It 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, was designed as 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.[47]

Others working on deepening research and innovation links between large companies, universities and start-ups in Australia include Data61 within CSIRO (see Box 7) and fintech hub Stone & Chalk, which recently floated the idea of a new Cyber Security Innovation Lab to promote collaborative research and development in the Australian cyber security industry.[48] The plans envisage the launch of the lab sometime later this year. Dimension Data and Deakin University have also announced a partnership to establish Australia's first dedicated cyber security incubator at the University's Waurn Ponds campus, with funding support from the Victorian Government's LaunchVic start-up initiative.[49] The incubator is due to open in 2017.

Box 7: Australia's digital powerhouse—Data61

Data61 was formed in 2015 when Australia's national IT research facility NICTA merged with the digital research unit of the country's chief science organisation CSIRO. Its mission: find and develop new "cutting-edge" technologies for today's data-driven world. Today, Data 61 is considered Australia's biggest research facility of its kind. With more than 1,100 staff spread across six states and territories, including more than 400 resident PhD students, it also hosts one of the largest data research teams in the world.

Scientists at Data 61 have developed insect-like legged robots whose sensors allow them to create a digital elevation map of an area. They have created new software tools to help analysts predict the behaviour of bushfires. And they are working on installing a vast wireless network of sensors and nodes in the Amazon region to help track the loss of animals and plants.

Cyber security is a key research focus for Data61. Recently, the group became the first worldwide to investigate a common security feature for Android mobile devices. Now that mobile phones are essentially mobile computers, millions of users worldwide are turning to so-called VPN (or Virtual Private Network) apps to hide their browsing activity, access region-restricted content and ensure their data is secure when using public Wi-Fi networks. Data61, in conjunction with researchers from UNSW and the University of Berkeley, revealed that these apps are not as secure as they make out to be. Another recent achievement was the development of a very small, yet powerful base system for computers and mobile devices—a so-called kernel—that equips operating systems with one of the world's strongest basic protection against viruses, trojan horses, ad-ware and spyware.

Underpinning the model of Data61 is its strong emphasis on research collaboration. The group is connecting academia, corporations, startups, governments, investors and entrepreneurs across the globe. For example, it has created a Data Research Network to link industry with data researchers and delivers data analytics training to businesses.

Smaller industry participants, however, have been slower in tapping university expertise for the development of new products and services. Interviews with a wide cross-section of local cyber security startups reveal that only two out of more than 22 are currently working closely with universities.[50]

While the Australian Government has picked cyber security as a national priority research area, there is not currently a Cyber Security Cooperative Research Centre (CRC). CRCs provide access to additional government grants and foster collaborative partnerships between industry and research organisations with the aim of improving the development and commercialisation of Australian technology. CRCs exist for a range of other fields, from Satellite Systems to Beef Genetic Technologies, and there is now broad support among industry for the establishment of a Cyber Security CRC to consolidate existing research capability and pursue collaborative research endeavours for national benefit.

In interviews, industry participants have acknowledged several barriers to greater industry research collaboration in Australia. Some executives admit that they lack experience in engaging universities to leverage their knowledge. Some also say that the diverging planning horizons—companies tend to focus on their immediate, short-term needs, while basic research occurs over longer timeframes—are limiting their close collaboration with academics. 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 (*Grow 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.

Access to capital to support innovation is limited

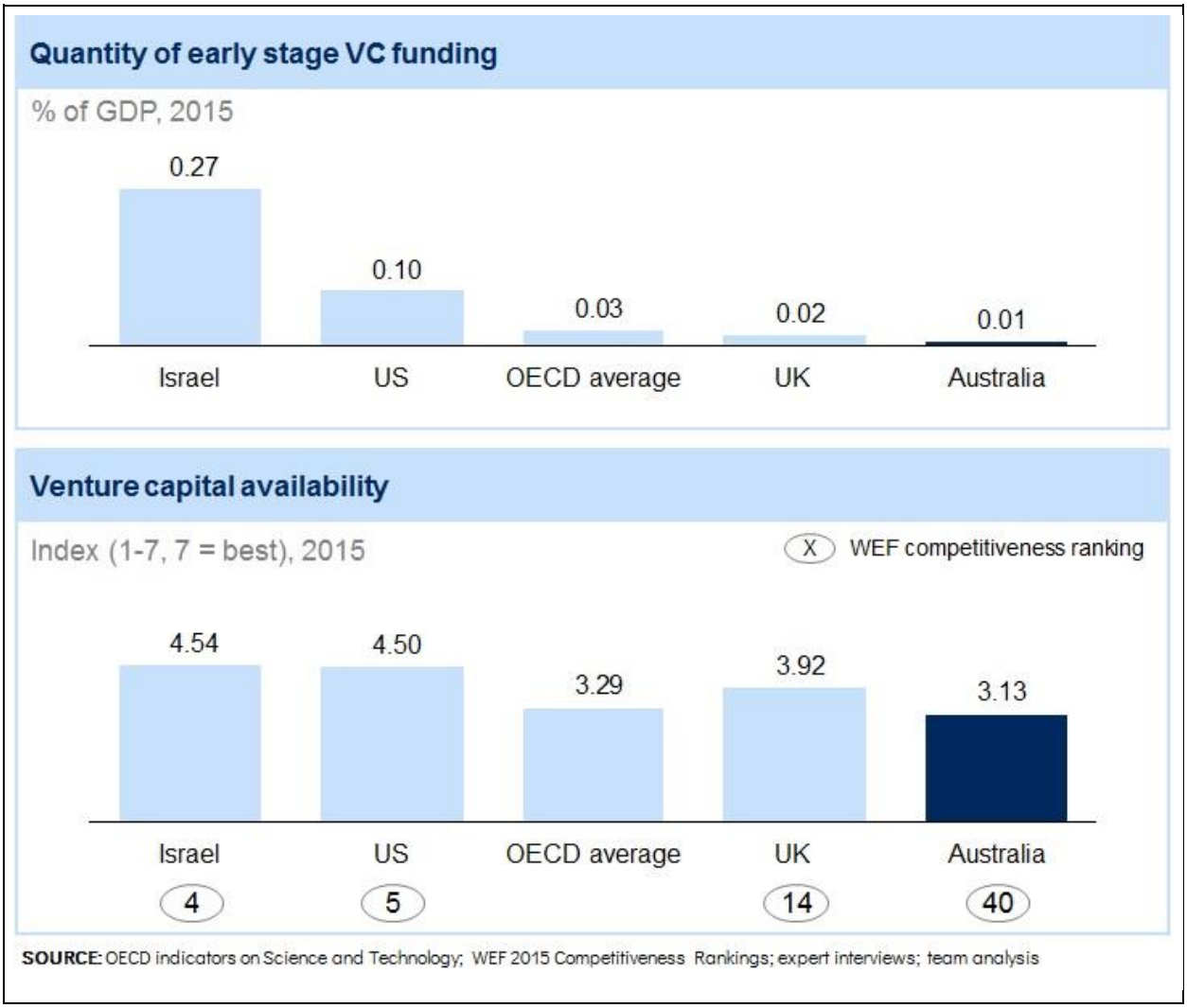
Venture capital (VC) funds investing in early-stage startups are currently scarce in Australia, noting there is some government assistance and incentives available. This low availability blocks the country's innovation pipeline because startups are locked out from the high-risk capital they urgently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

> **"Cyber security is [...] perceived as a risky and technically complex business. VCs 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

OECD data comprised in Exhibit 22 show 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 those countries are considered leaders in the global market for cyber security products.

Data compiled by the World Economic Forum and shown in Exhibit 22 further highlight the difficulties Australian startups are facing when trying to tap VC funding.[51] On a scale from 1 (hard) to 7 (easy), Australian executives surveyed for 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.

Exhibit 22:



This problem of access to early-stage VC funding is well known and acknowledged by the Government in its assessments of the Australian innovation system.[52] A number of recent policy measures have attempted to address this through tax concessions. The Government in 2016 also launched the CSIRO Innovation Fund, which aims to fill this funding gap by co-investing in spin-offs, startups and SMEs engaged in the commercialisation of early stage innovations.

Cyber security startups, however, might face bigger obstacles than their peers because they offer complex, highly technical products. Most Australian VC funds are generalists by necessity because of the limited market size, as opposed to the US where there are several VC funds with expertise in cyber security (e.g., Rally Ventures). Interviews with Australian cyber security professionals indicate that local VC fund managers perceive the cyber security industry as complex and risky, and are reluctant to invest because of a lack of expertise in this field.

> **"Pitching to early-stage VCs 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

Various approaches to this issues are discussed in Chapter 4.1 (*Grow an Australian cyber security ecosystem*), including familiarising new investor groups, such as superannuation funds, with investment opportunities in the local cyber security industry.

3.3 Firm 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 firms succeed and our industry develops. Firms 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.

Capability gaps and market barriers make it hard for firms to grow in Australia

Interviews with buyers of cyber security and the Australian firms that provide these products and services signal that 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.

Box 8: 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 all 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 our capabilities for economic benefit and establish a globally attractive cyber security ecosystem.

Common themes are threaded through the journey of these companies. Years ago, all three left Australia in order to access high risk early stage capital; be in close proximity to business mentoring and growth support networks; and grow their customer base. All are based in Silicon Valley, with Dtex Systems landing there after exploring market opportunities in South East Asian and the United Kingdom. In 2017, these Australian success stories are all now establishing business units in Australia, mostly in R&D and sales support, as part of global growth strategies.

All are optimistic about Australia's future as a cyber security leader and offer some perspectives on the sector.

Casey Ellis from Bugcrowd sees the Australian market improving for startups as high value talent and increasing levels of investor capital start to flow. Casey recognises Australians have many strengths and that organisations, including Bugcrowd, want access to the talent of that "Australian DNA" that makes our cyber security professionals so attractive, stating "Australia is world class at troubleshooting, the world knows it but Australia doesn't - yet." 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 that Australia is now in a position to seize opportunities in the global cyber security industry and this will generate economic growth for Australia over the next five to ten years, stating "Australia can be a centre of cyber excellence for the region." For this to occur, he believes the mindset of Australian businesses and the Government must evolve to be less conservative by encouraging innovation and buying local cyber security solutions. Mohan also sees Australian universities playing a crucial role in fostering the growth as part of maturing the ecosystem.

Hamish Hawthorn from UpGuard 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 refers to building a domestic capability being key to developing a vibrant cyber security ecosystem. Hamish attributes his time in Silicon Valley as being beneficial to developing and strengthening the product they now offer, largely due to the intensity of the competition in the US market but also the Silicon Valley ecosystem encouraging fast learning through iterative development of solutions. This process of innovation is something he believes can be achieved in Australia through continued cultural change and greater risk tolerance for emerging technology.

Cyber security firms need to understand their customers

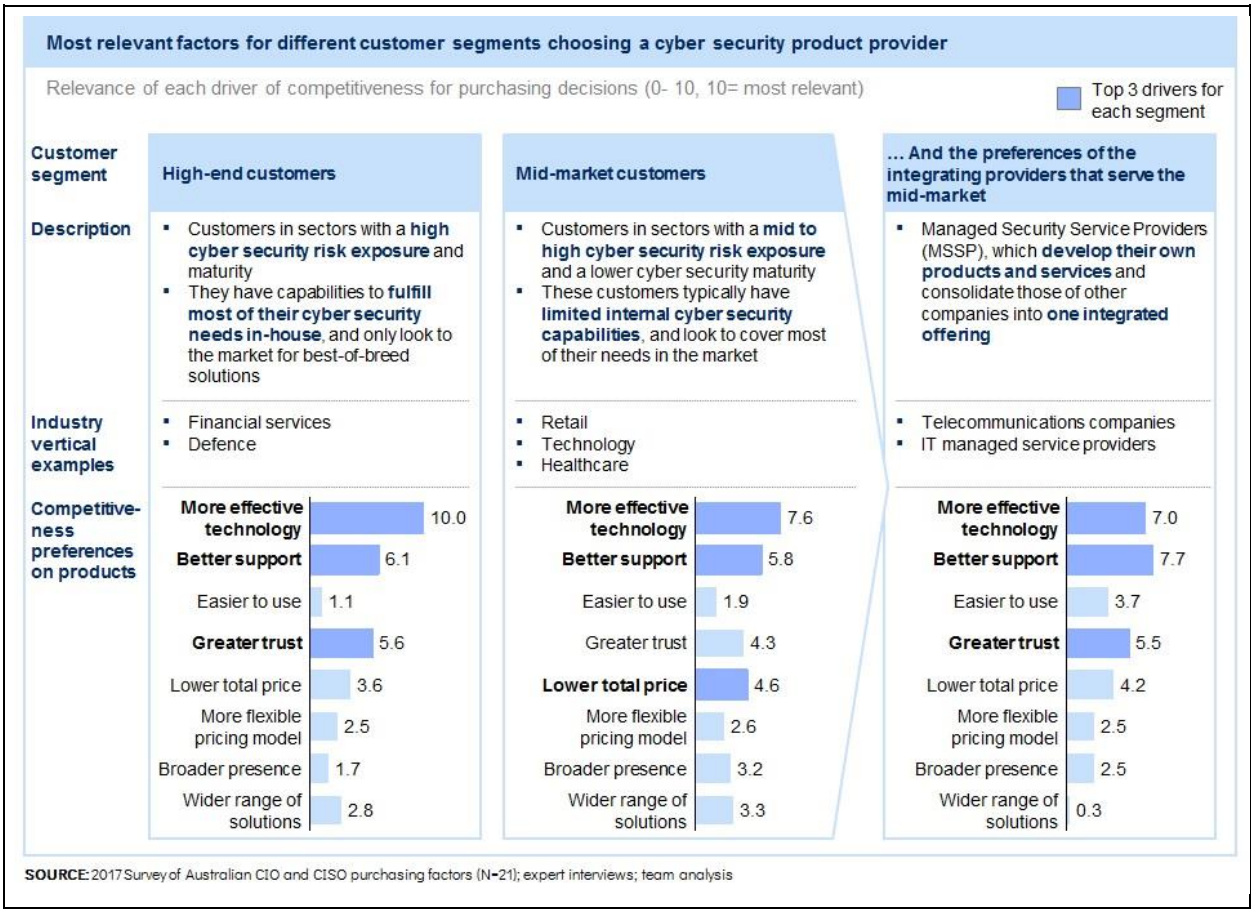
The AlphaBeta/McKinsey survey of CIOs/CISOs and local cyber security providers indicates that many Australian cyber security firms tend to undervalue aspects of their offerings that are critical for local customers. This mismatch is most evident for customer support, according to the survey results listed in Exhibit 23. When purchasing products, customers consider support to be an essential component of their purchasing decision, while local firms are more focused on providing a user-friendly service. A greater understanding of and focus on local customer needs would likely help Australian cyber security firms grow (described at Box 9 as one example).

Exhibit 23:

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

Additional survey results shown in Exhibit 24 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 firms 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 with the greatest trust, best support and most effective technology on offer.

Exhibit 24:



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. They are also more cost-conscious than other customers in the market, the survey shows.

Firms also need to consider if their product or service might be better targeted not at an end-user customer but at an integrator, such as a Managed Security Service Providers (MSSP). MSSPs are typically focused on serving 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. Telecom companies are one example for 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.

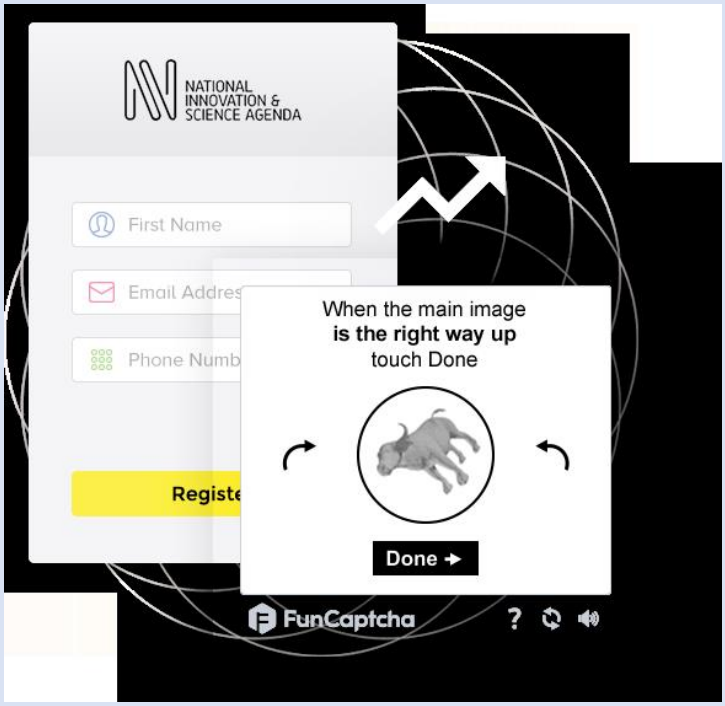
Box 9: Homegrown startup changing up human verification online

"Completely Automated Public Turing Test to tell Computers and Humans Apart" or CAPTCHA is used to protect websites from spammers. Most available CAPTCHAs require the user to read and type in text, which is often difficult to read—so that the CAPTCHA is effective against the sophisticated range of bots. This verification process becomes annoying for the user and as a result, the user can end up leaving the website.

FunCaptcha have created a unique way to manage the online verification process by engaging users with fun and effective visual puzzles to solve so the website can distinguish automated attackers from human users on the internet. The startup distinguishes itself from traditional CAPTCHAs by using fun visuals during the verification process and by adjusting its security vetting process based on the number of users and how they interact with the CAPTCHA. The solution eliminates the threat of an automated attacker with their enterprise-grade security that is backed by patent-pending technology and a team of experts.

Founded in Brisbane in 2013, FunCaptcha already has a presence in 100+ countries. FunCaptcha's customer base is seeing strong growth among some of the world's most trusted brands' websites, mobile apps and games to tackle spam, ticket scalping, account fraud, brute forcing or an entirely new attack. After spending a lot of time researching the Australian market, FunCaptcha identified opportunities in the US market due since a large portion of websites that Australians use are built and hosted of the US. FunCaptcha attribute their early success in entering the international markets by attending US security conferences as a platform to build a strong referral network.

The founders of FunCaptcha are driven by their natural curiosity to embrace any discovery and have extensive experience successfully designing, developing and selling gaming technology.

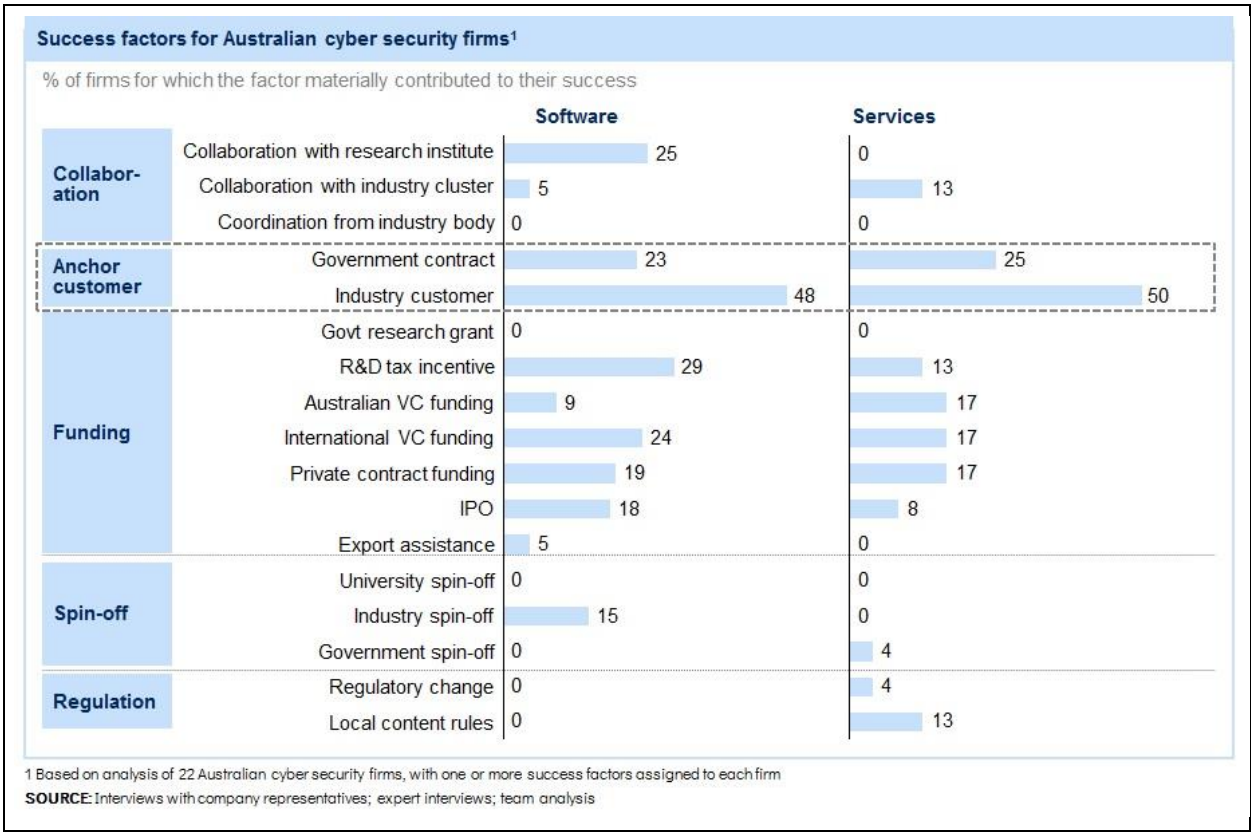


New firms struggle to develop the trust needed to gain anchor customers

A range of local cyber security firms were analysed to understand which factors—including funding, R&D collaborations and industry regulation—were most important for their development and success. The results shown in Exhibit 25 highlight that acquiring an "anchor customer" ranks as the most commonly cited success factor for Australian cyber security firms.

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 start-up 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. The survey results show that Australian cyber security firms most commonly relied on an anchor customer from industry (relevant for approximately half the firms surveyed), while about a quarter of the firms surveyed said a government contract was critical to their success.

Exhibit 25:



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 firms reveals that trust is a crucial factor, particularly when selecting service providers.[53] And while buyers of cyber security products, such as antivirus

software or firewalls, are generally most interested in buying the most effective technology, Exhibit 26 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 firms 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.

Exhibit 26:

> **"A common concern around local firms 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

Large potential customers may remain reluctant to engage if a firm has no track record to indicate that a new product or service will deliver the promised outcome. Interviews with CISOs in Australia reveal that many hesitate buying from smaller or newly established providers with no reputation, even if these firms offer technologically appealing products. Potential customers may also question

the financial health of a cyber security start-up and seek evidence that it will exist long enough to support its products and services well into the future.

Box 10: Select accreditation programs for Australian cyber security firms

The Australian Signals Directorate (ASD), an Australian Government intelligence agency in the Department of Defence, evaluates and certifies ICT products and services that meet the high-level security standards of Government agencies, making it a go-to address for any cyber security firm wishing to win a government agency as customer. The ASD currently has several certification and accreditation schemes in place that businesses can join to bridge a gap in trust:

- Australasian Information Security Evaluation Program (AISEP) – The program assesses whether ICT security products and systems work correctly and effectively and do not show any exploitable vulnerabilities. Products and systems that pass this test are added to an Evaluated Products List, which approves of their use in Australian and New Zealand government agencies and certifies them against international standards. The program reviews a range of products from data and network protection to security modules.
- Service certification – The ASD tests and certifies the effectiveness of certain ICT services, in particular gateway services, which seek to prevent malicious web traffic from entering the network of an organisation, and cloud services. Australian Government agencies are strongly discouraged from working with uncertified cloud or gateway security service providers to protect government information.
- Information Security Registered Assessors Program – This program trains and accredits individual cyber security professionals to undertake assessments of organisations' security compliance and highlight information security risks, with a focus on compliance with Australian Government information security standards and requirements. The Council of Registered Ethical Security Testers Australia New Zealand (CREST), a not-for-profit based in Canberra, is another entity that assesses, accredits and certifies cyber security professionals and firms in Australia and New Zealand. Its accreditation scheme is limited to firms providing penetration and vulnerability testing services, i.e. screening a computer system, network or web application for vulnerabilities that an attacker could exploit. A CREST membership comes at a cost of A$10,000 per year and it takes a maximum of six months to obtain a CREST certification.

> **"Bizarrely, firms have found it easier to gain contracts in the US than in Australia, due to a lack of willingness of Australian companies to embrace them."**
> —SINET61 2016 conference brochure

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.

One way for firms to overcome the lack of trust is to use one of several certification and accreditation programs available in Australia (see Box 10 for further details). Another, perhaps surprising, way to overcome local market barriers is to expand overseas. Some local cyber security firms 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 firms illustrates the widespread risk aversion in the local market.

Chapter 4.1 (*Grow an Australian cyber security ecosystem*) outlines a range of 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.

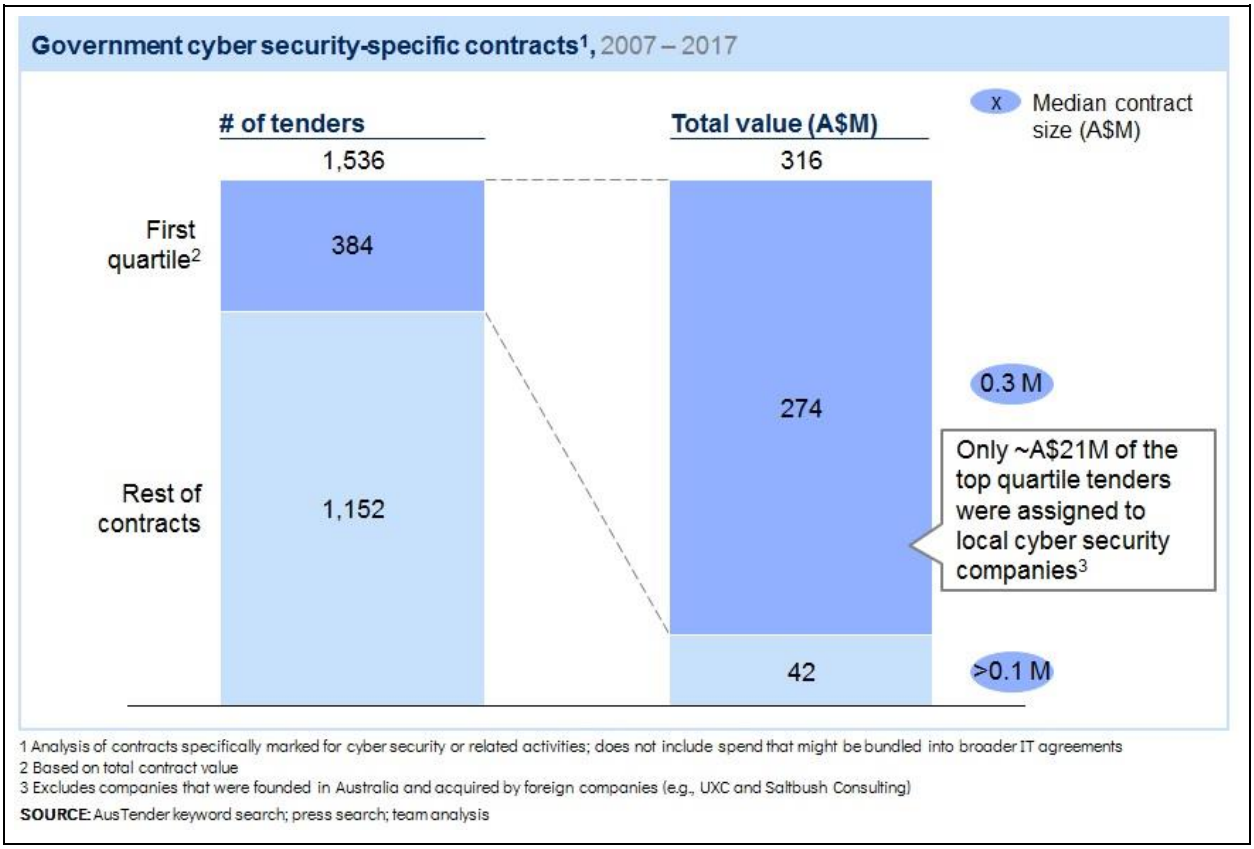
Procurement processes favour larger, established firms

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 firms lack the resources to deliver large-scale projects, particularly when they cover multiple product and service areas like 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 that is 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, comprised in Exhibit 27, 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 eight per cent of these high-value government contracts were concluded with local Australian grown and owned firms, as most of them are still too small to effectively compete against large foreign rivals in a government tendering process.

Exhibit 27:



The large-scale contracts commonly offered by Australian government agencies—a median size of A$300,000 for the top quarter of contracts—are 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.

> **"Big organisations tend to hire big organisations."**
> —CIO of an Australian bank

Research shows, for example, that the share of small and medium-sized firms securing government tenders in European Union countries rapidly declines once the overall contract value rises above A$150,000.[54] 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 firms to service different aspects of their security needs. Of course, purchasing from more providers could also make systems more complex and less integrated, so any move to smaller contracts would need to be properly weighed against such potential complications.

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 in the Federal Government 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 of 170 suppliers and has been used to procure some cyber security-related contracts.[55] The current panel was appointed in 2013, and there will be no new opportunities to join this panel until it expires in 2019.

The Australian Government is trying to remove barriers to entry. This year, it has added new features to its Digital Marketplace—an online platform for buyers and sellers of various ICT products and services—and opened it up to cyber security businesses, making it easier for them to work with Australian Government agencies. The Digital Marketplace uses a strict selection process for firms wishing to use the platform for their offerings. Similarly, cyber security services firms must demonstrate certain abilities and experiences before they can join the Digital Marketplace.[56]

Importantly, the Digital Marketplace could also provide cyber security firms with access to state and local government buyers. The NSW government has already announced that the Marketplace is compliant with its procurement policies, and it will begin purchasing some ICT services through the new platform.[57] 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 firms.

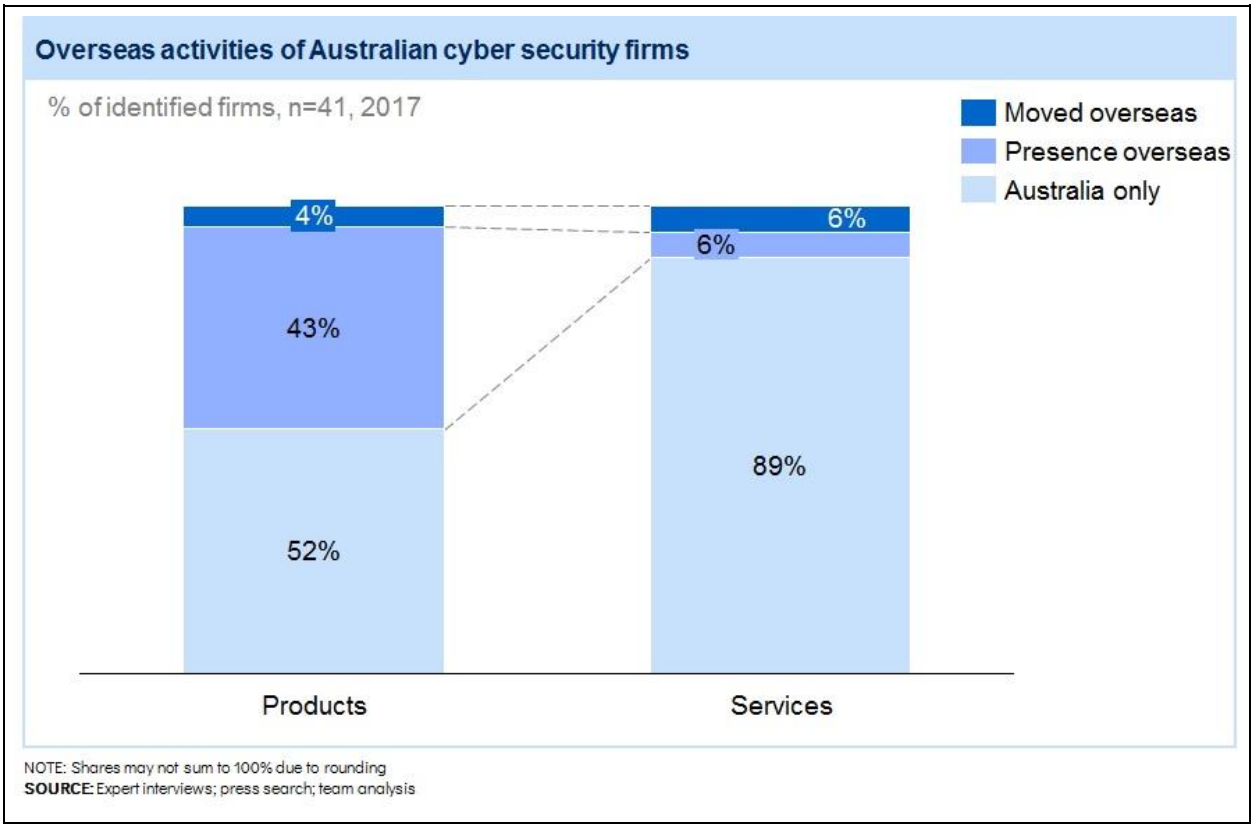
Many of these issues in public sector procurement are also common to private sector procurement processes, which are often deliberately designed to weed out startups and smaller firms through narrow evaluation and review criteria. The preference to work with larger players is particularly strong in cyber security, which affects highly sensitive parts 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 likely remove some of the substantial hurdles that cyber security startups are facing. For more details on recommended actions to address this issue, see Chapter 4.1 (*Grow an Australian cyber security ecosystem*).

Australian cyber security firms struggle to access global export markets

An analysis of the geographical spread of Australian cyber security firms reveals significant scope for the industry 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 firms in the Australian cyber security industry have not yet developed an export capability. In fact, Exhibit 28 reveals that only 12 per cent of Australian cyber security services firms surveyed have customers outside of Australia.

Exhibit 28:



Of course, 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 firm, 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 the jobs created are predominantly in Australia. How firms design their service offerings can have a major impact on their exportability, and some Australian cyber security firms 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 firms indicated that, for them, exporting is not a priority simply because they already struggle to recruit enough cyber security professionals to meet strong domestic demand.

Chapter 4.2 lists several strategies that could help overcome some of the common export issues Australian cyber security firms are facing, such as intensifying Australia's marketing presence for cyber security in key target markets and analysing remote delivery models for Australia's existing services strengths.

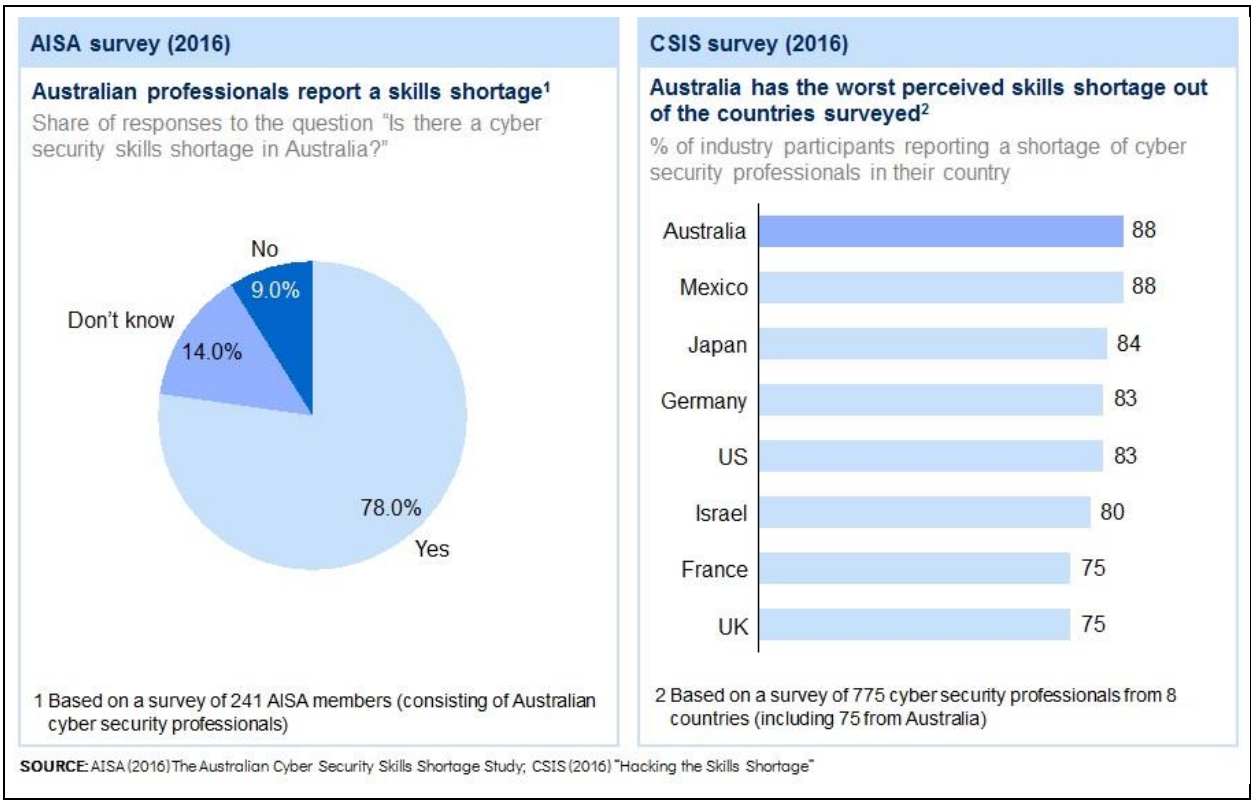
3.4 Skills and workforce

A strong and well-trained workforce is critical to Australia's ability to capture the growth opportunity presented by the rapid increase in demand for cyber security. Yet there are signs that Australian cyber security firms are struggling more than their global peers to attract the right talent for their businesses. The lack of job-ready candidates, caused by the inability of formal education providers to rapidly produce more cyber security graduates and the failure of many workplaces to offer on-the-job training, is a major challenge for the cyber security industry, as this chapter will show.

The cyber security industry is grappling with a skills shortage

In 2016, three out of four local cyber security professionals surveyed by the Australian Information Security Association (AISA) said a skills shortage is plaguing their industry, as shown in Exhibit 29.[58] 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 industry is one of the worst in the world: 88 per cent of Australian cyber security professionals observe a skills shortage in their industry. Only Mexican professionals share similarly dire views, as shown in Exhibit 29.[59]

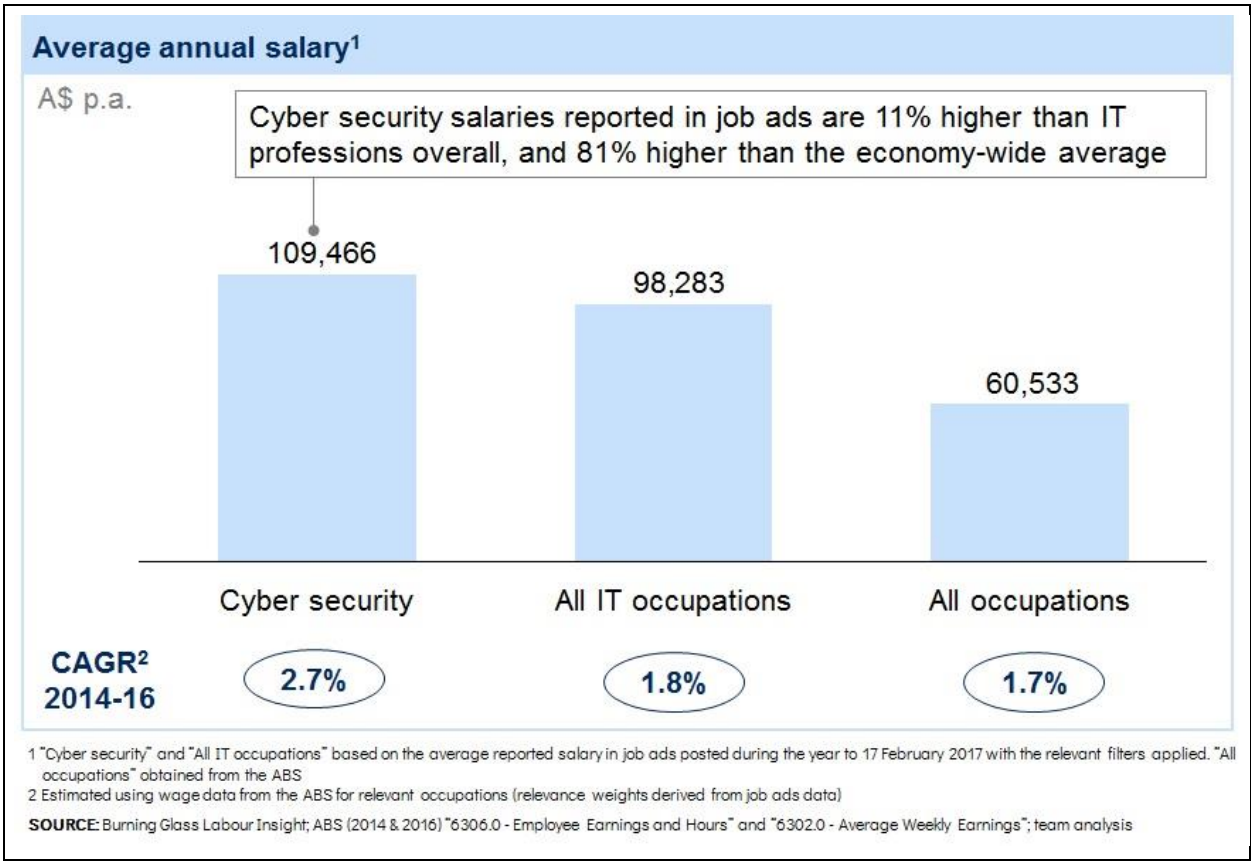
Exhibit 29:



Interviews with company executives, government officials and other stakeholders echo the perception that the Australian cyber security industry is grappling with an acute talent shortage. Wage premiums paid by cyber security firms in Australia to attract and retain employees are symptomatic of the lack of available skills.

Exhibit 30 reveals that cyber security workers in Australia earn 11 per cent more money than the average IT worker and 81 per cent more than the average Australian. This is slightly higher than the US, where the premium for cyber security salaries over IT salaries was nine per cent in 2015.[60] Salaries in cyber security are also rising faster than in other occupations. Between 2014 and 2016, the average wage of a cyber security worker in Australia increased by 2.7 per cent per year—compared with an average annual wage growth of 1.7 per cent in the wider IT industry and 2.0 per cent in the Australian economy overall.

Exhibit 30:

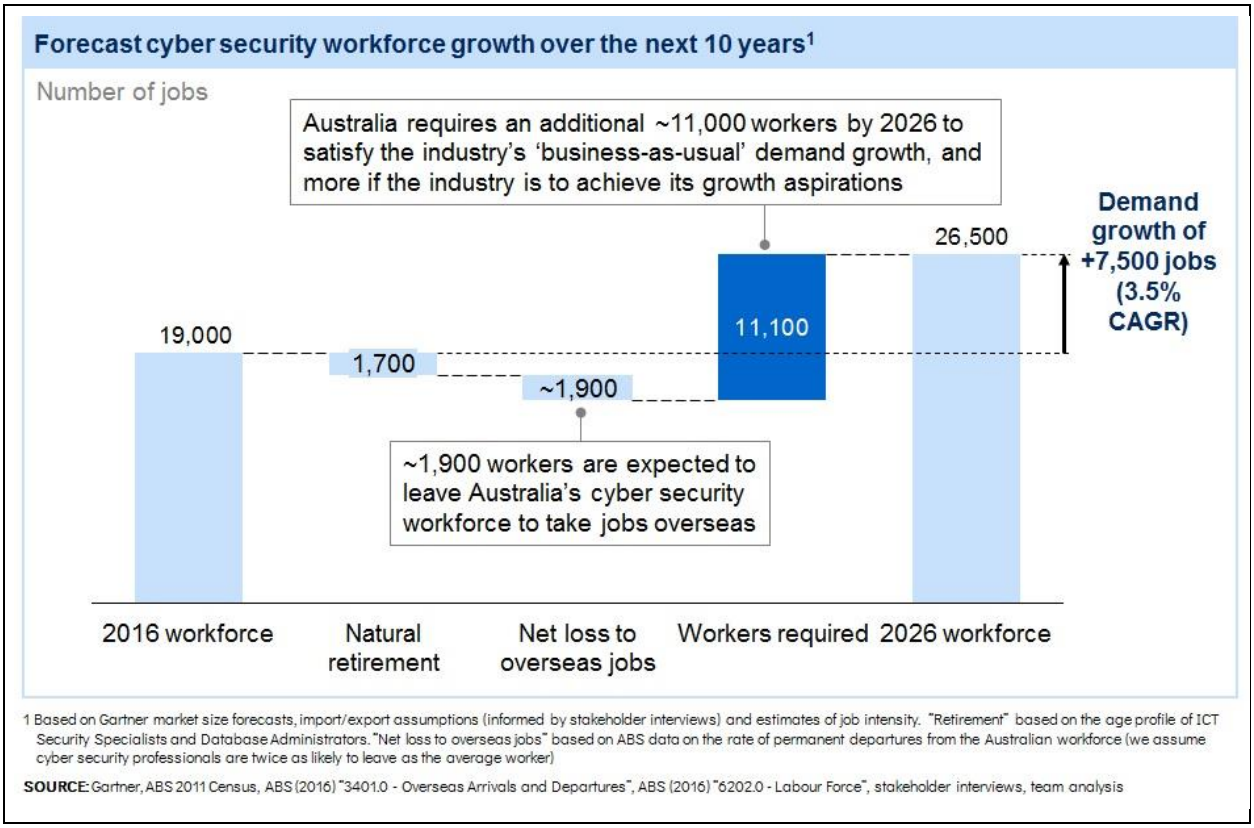


A shortage of skilled cyber security workers causes direct economic damage. Every third firm surveyed by the Centre for Strategic & International Studies and Intel Security says the lack of specialised cyber security staff makes them a more likely target for cyber adversaries who seek to exploit any vulnerabilities, and 25 per cent of respondents said their organisation has lost proprietary data through a cyber attack due to the skills shortage.

While the skills shortage is already visible, modelling of future workforce needs indicates the challenge may become significantly more severe. A detailed analysis based on current labour-market trends suggests that the Australian cyber security industry will need to increase in size by 7,500 workers by 2026—implying an average growth rate of at least 3.5 per cent per year—just to meet the forecast future demand.

Exhibit 31 shows that the gross demand for new workers is likely to be closer to 11,000, however, because Australia is expected to lose several thousand of cyber security professionals over the next decade, either due to retirement or to jobs overseas.[61]

Exhibit 31:



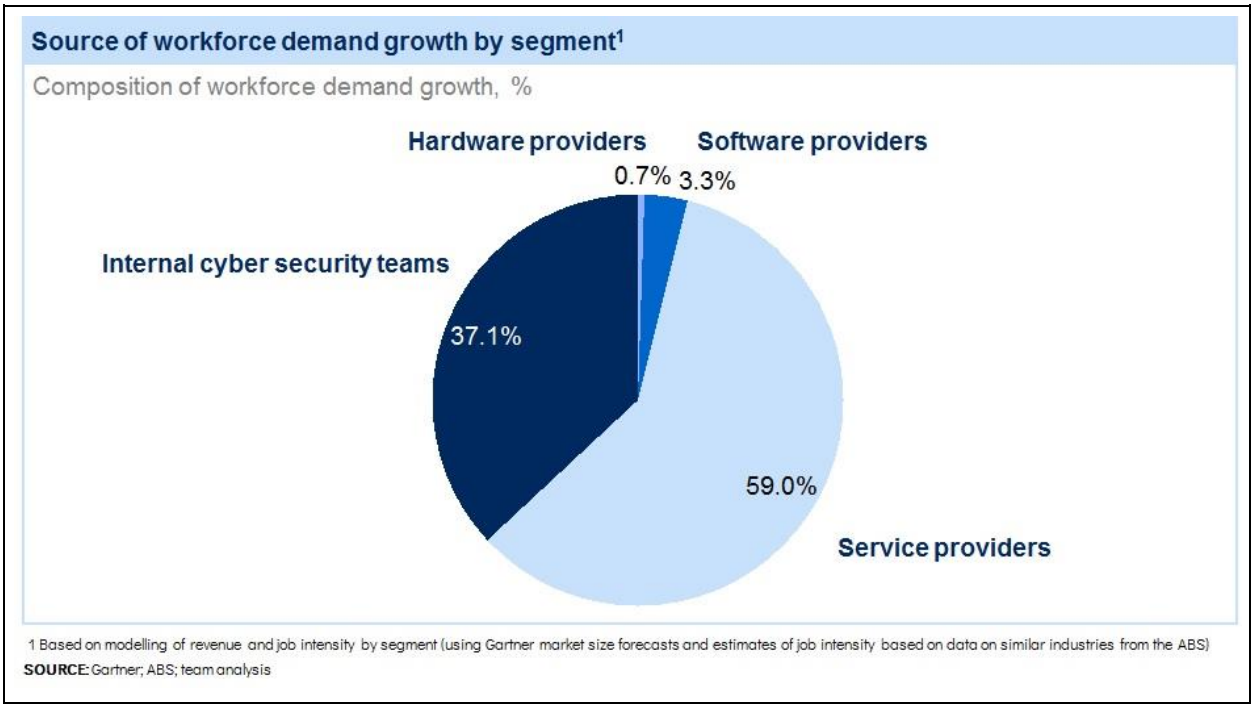
1 Based on Gartner market size forecasts, import/export assumptions (informed by stakeholder interviews) and estimates of job intensity. "Retirement" based on the age profile of ICT Security Specialists and Database Administrators. "Net loss to overseas jobs" based on ABS data on the rate of permanent departures from the Australian workforce (we assume cyber security professionals are twice as likely to leave as the average worker)

SOURCE: Gartner, ABS 2011 Census, ABS (2016) "3401.0 - Overseas Arrivals and Departures", ABS (2016) "6202.0 - Labour Force", stakeholder interviews, team analysis

Most of Australia's future demand for cyber security workers will be driven by the services segment, which is in line with the overall growth profile of the industry, Exhibit 32 shows.

External cyber security services firms could absorb more than half (59 per cent) of all additional workers needed in the cyber security industry by 2026, Exhibit 32 illustrates. Meanwhile, government agencies, banks and other highly-risk sensitive firms are expected to drive around 37 per cent of the growing cyber security workforce demand in Australia, as they seek to bolster their internal IT security teams over the next decade. Hardware and software manufacturers are forecast to require the smallest number of additional staff, which reflects the smaller size and lower labour intensities for those product types.

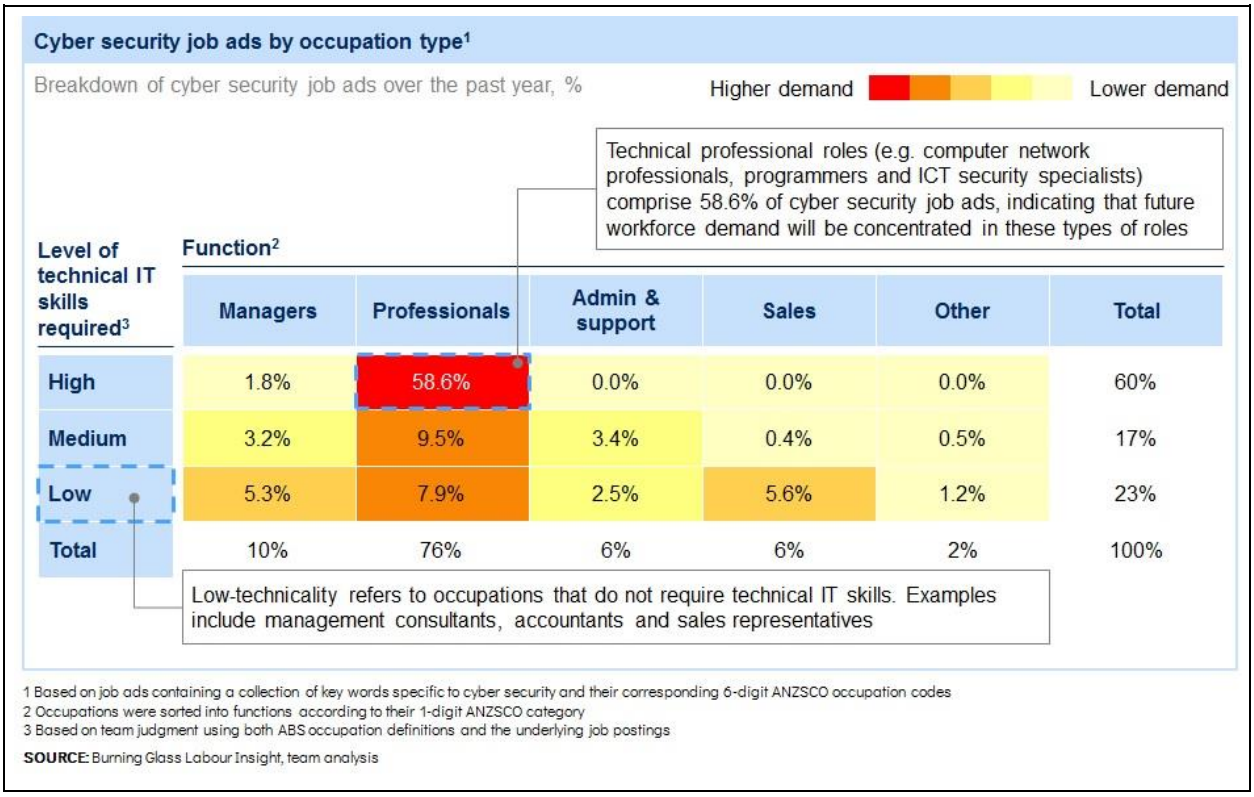
Exhibit 32:



Understanding the diversity of the workforce is an important element of addressing the skills shortage. There is a tendency to think that the cyber security workforce consists only of highly technical professionals. However, this is not the case, Exhibit 33 reveals: in the past year, just over half (58.6 per cent) of job advertisements for cyber security were for high-technicality IT professionals.

These technical professionals work across all industry segments and comprise occupations such as computer network professionals, programmers and ICT security specialists. Almost 20 per cent of demand in cyber security is for medium or low-technicality professionals, including lawyers, accountants and teachers. A further 24 per cent of job advertisements are for non-cyber security professional roles such as admin, sales and management. While demand for different types of workers will of course shift over time, this assessment of recent trends provides a reasonable gauge of the future demand patterns.

Exhibit 33:



The formal education system is not producing enough job-ready candidates

The good news first: Australian universities and vocational institutions are already working on alleviating the acute skills shortage affecting the cyber security industry. Interviews with various university representatives indicate that the pipeline of graduates with relevant skills is growing.

In 2015, close to 13,500 students acquired a general IT degree in Australia.[62] They would be suited to work as cyber security professionals if they completed some additional training. At the same time, the array of specialised study opportunities have expanded as universities have begun to respond to the need for talent by offering tailored subjects and degrees. For example, Deakin University offers both a Bachelor and Masters of Cyber Security, while Edith Cowan University (ECU) has a Bachelor of Science (Cyber Security) and a Masters of Cyber Security. UNSW Canberra has a suite of Masters programs in cyber security with varying levels of technicality. Several other universities are offering cyber security as a major within their basic IT or computer science bachelor degree programs.

Universities have also entered into partnerships with industry in order to accelerate their teaching capacity. In 2016, Macquarie University and Optus announced a co-investment of A$10 million to establish a Cyber Security Hub that will offer several degree programs at undergraduate and postgraduate level (see Box 11 for further details). This follows a partnership announced in late 2015

by the Commonwealth Bank of Australia and UNSW called sec.edu.au, which aims to deliver, among other things, a comprehensive cyber security specialisation as part of UNSW's computer science degree.

Box 11: Businesses and universities join forces to bridge the skills gap

A recent series of high-profile security breaches in Australia has put business leaders on the alert. Malicious cyber actors are launching increasingly sophisticated attacks on corporate data networks, compromising a growing range of targets—airports and power grids, retailers and credit card firms, and even the national weather bureau. But as threats are multiplying, most businesses remain vulnerable. They lack the expertise to identify and manage mounting security risks, and many are struggling to find help amid a severe skills shortage in cyber security globally.

While the Australian Government's Cyber Security Strategy acknowledges the urgent need to address this skills shortage, some leading Australian companies have recently begun to tackle the challenge themselves. Late last year, Australian telecommunications firm **Optus** entered an alliance with **La Trobe University** in Melbourne to co-develop a new tertiary degree in cyber security.[63] The partnership will invest up to A$8 million to turn the university's existing campus into a digitally connected learning and research precinct. It will also fund a new chair of cyber security to help Australia become a leader in cyber security research and teaching.

In a similar move, Optus has joined forces with **Macquarie University** in Sydney to create a new cyber security training and education hub, which brings together industry experts and university academics in a bid to grow Australia's cyber security talent pool. The A$10 million project includes a new cyber security degree for university students, as well as executive and business short courses. Optus uses these training courses to equip its own employees, and those of enterprise and government customers, with the latest cyber security skills and expertise.[64] "By collaborating with industry to tailor our study programs, we give our students a head-start in their careers, placing them at the top of Australia's cyber security talent pool," said David Wilkinson, Deputy Vice-Chancellor at Macquarie University.[65]

The announcement came after the nation's largest bank, **Commonwealth Bank of Australia**, teamed up with the **University of New South Wales** to boost the number of cyber security professionals and cyber security teachers in Australia. The bank has A$1.6 million over five years to develop a "centre of expertise for cyber security education", complete with an overhauled study curriculum and a new lab for experimental, hands-on teaching of cyber skills.[66] It has also begun to award a cash prize, the **Commbank Cyber Prize**, to Australia's best and brightest cyber students with the goal of enthusing more young people for a career in cyber security.[67]

In the near term, however, the pipeline of job-ready graduates will not reach the critical mass needed to mitigate the cyber security industry's skills shortage and enable future growth—even when accounting for these newly established cyber security study programs.

For one, the volume of cyber security students is still too low. While it is difficult to clearly define what constitutes a cyber security qualification (some students may only study a few cyber security-specific subjects within their degree program), interviews with universities suggest that currently about 300

students are graduating annually with undergraduate cyber security degrees, and a further 200 with postgraduate qualifications in cyber security. Even if new courses coming online were to add a further 200 graduates annually in the next few years, demand projections suggest that this would not resolve skills shortages.

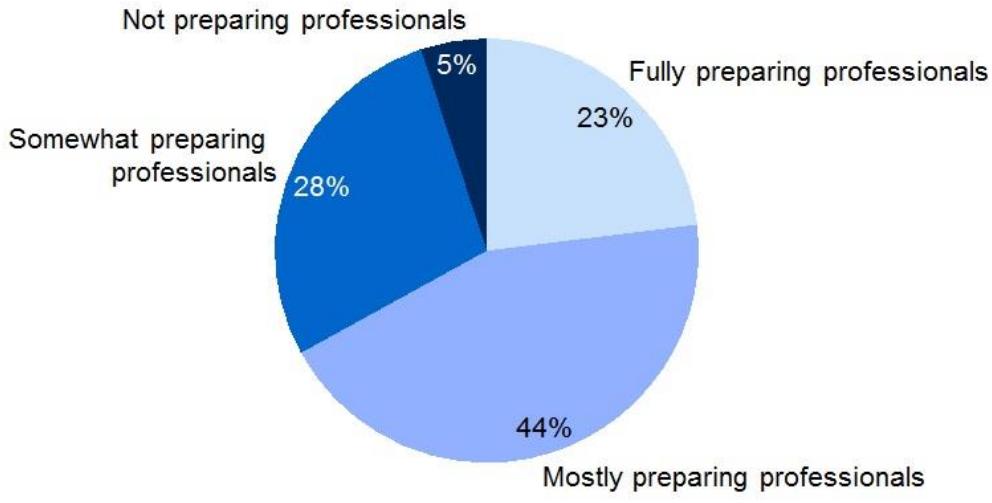
A shortage in teaching staff adds to the problem and prevents a rapid expansion of the graduate pipeline. Partnerships with industry and government may help ameliorate this situation somewhat; Commonwealth Bank through sec.edu.au is offering four fellowships for teaching staff at UNSW, while other industry partners are providing adjunct lecturers to universities from amongst their professional staff. CERT Australia provides teaching support for some courses at Edith Cowan University and Queensland University of Technology. However, supplying more qualified teachers to universities seeking to expand their cyber security offerings will remain difficult.

Secondly, industry participants are questioning the employability of many graduates. While Australian universities offer an increasing number of cybersecurity, several company executives have mentioned in interviews that graduates could be better prepared for the workplace. The issue extends beyond Australia, as Exhibit 34 proves. Globally, more than three-quarters (77 per cent) of cyber security professionals surveyed by CSIS and Intel Security think the industry's current training and education programs are not fully preparing professionals for the workplace reality, leading to calls for academic programs to incorporate more practical learning.[68]

Exhibit 34:

Effectiveness of educational programs[1]

Breakdown of responses to the question "How well do you think educational programs (universities or vocational) are preparing cybersecurity professionals for the industry?"

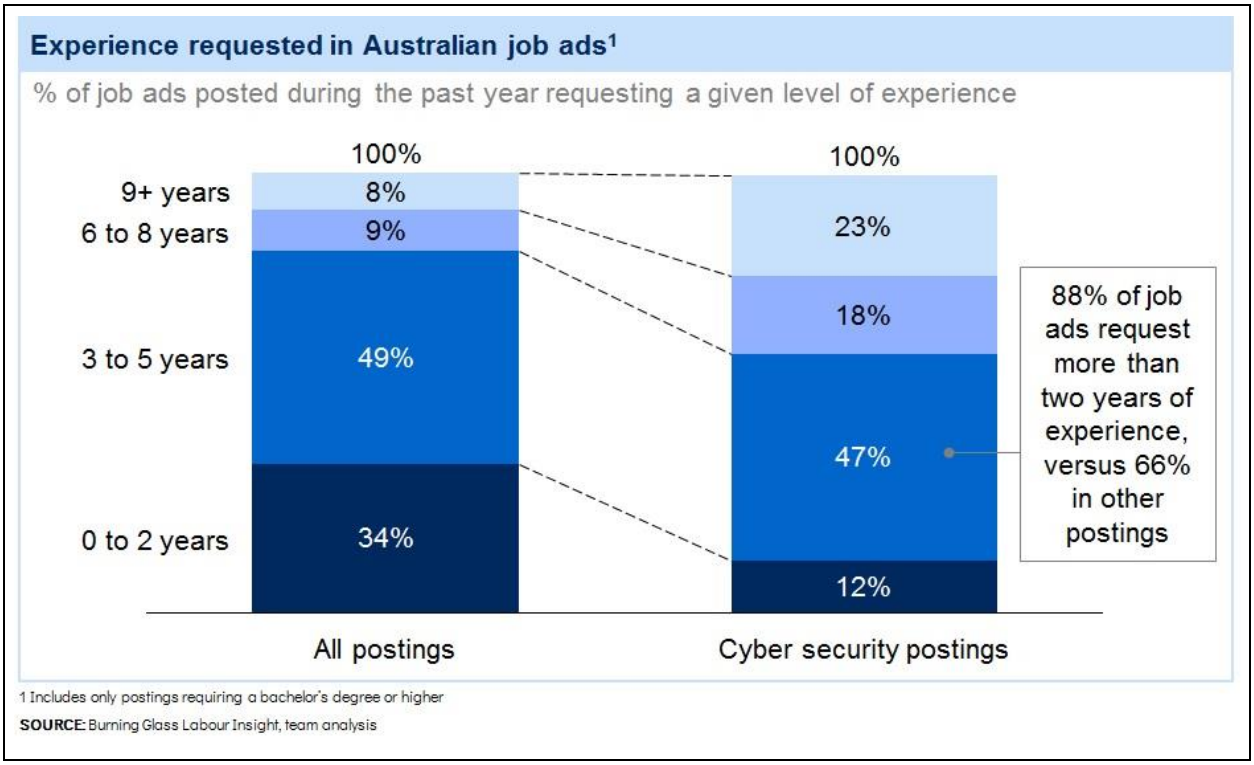


1 Based on a survey of 775 cyber security professionals from 8 countries (including 75 from Australia)

SOURCE: CSIS (2016) "Hacking the Skills Shortage"

Part of the dissatisfaction might stem from outsized expectations. Employers looking for cyber security staff typically demand a relatively high level of work experience. In 2016, almost nine out of ten cyber security job advertisements requiring tertiary qualifications also requested applicants to have at least two years of work experience, reveals Exhibit 35.

Exhibit 35:



> **"Candidates often have many certifications, but cannot effectively engage with business or other technical staff in order to complete their roles."**
> —response to the 2016 AISA Skills Survey

Employers in other areas of the Australian economy tend to set the bar much lower. Only two-thirds of economy-wide job ads targeting applicants with bachelor degrees ask candidates to have work experience of three years or more. New graduates typically also require some practical training before they're considered ready to perform on the job. However, opportunities for on-the-job training in the cyber security industry are sparse, which aggravates existing bottlenecks in the supply of workers.

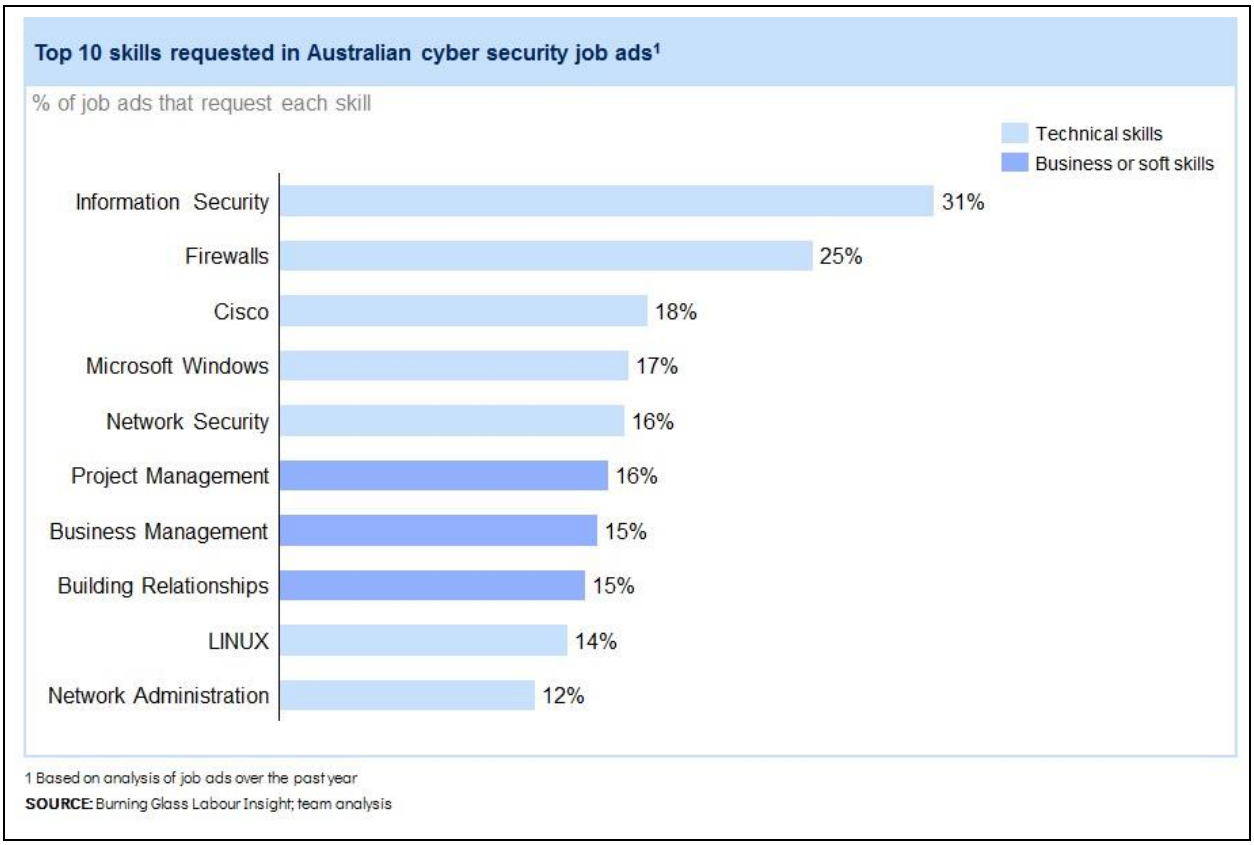
Companies with large cyber security teams—mostly big banks and professional IT services firms—have the capacity to train candidates from varied backgrounds. But limited resources currently prevent the large number of small and medium-sized companies (and even some of the larger corporates with smaller IT security teams) from offering extensive training for new hires. Many prefer

to search for highly experienced candidates instead. This may also reflect a broader reluctance of employers to invest in workplace training, as employees change firms more often in today's economy.

> **"Whether there is a skills shortage depends on who you are. We had the resources to train people from a variety of backgrounds and could pay to attract good candidates. But if you're a smaller team, you will struggle."**
> —CISO of an Australian bank

Another often-cited criticism is a lack of soft skills among graduates. Cyber security professionals, in addition to being technically versed, need to be able to manage projects and build relationships, as illustrated in Exhibit 36. Yet, interviews with industry professionals signal that many graduates lack such skills.

Exhibit 36:



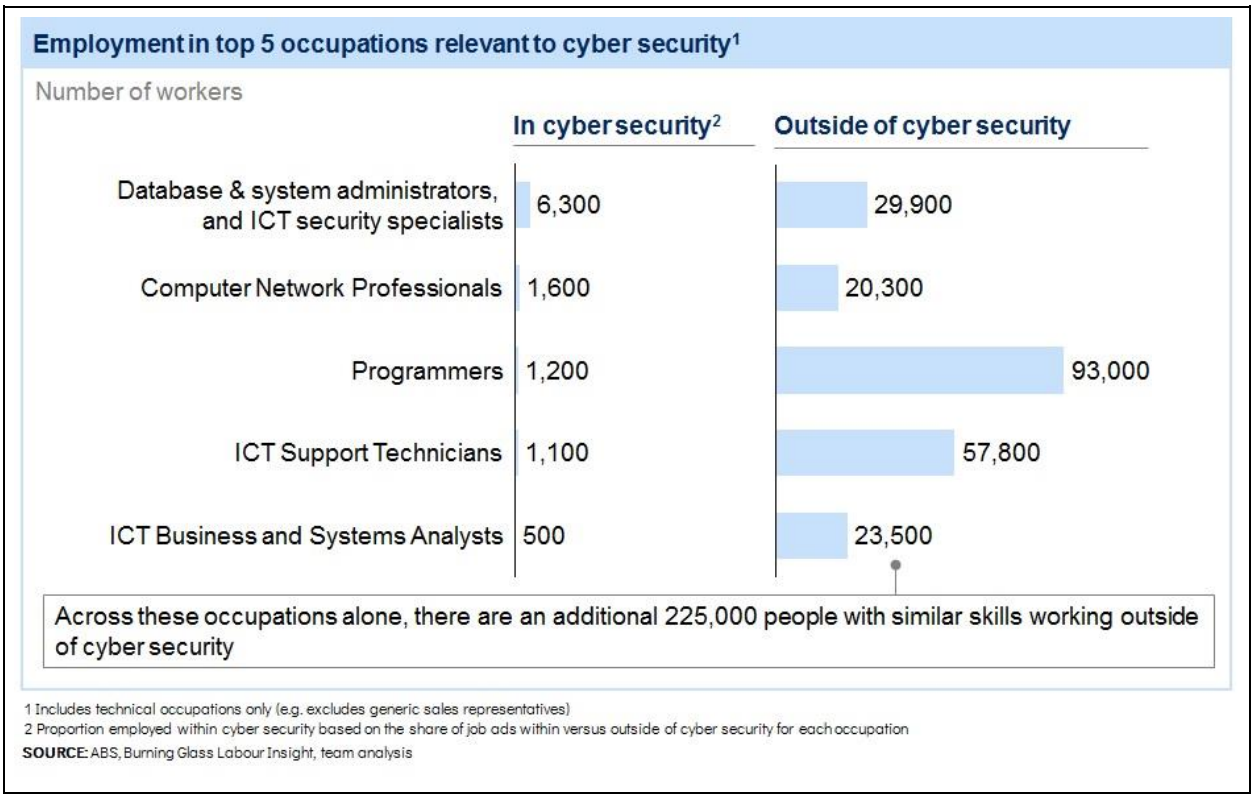
Chapter 4.3 (*Make Australia the leading centre for cyber security education*) outlines a range of actions to improve the number of job-ready cyber security professionals emerging from the formal education system, including developing further industry partnerships and expanding awareness of cyber security careers in high schools.

Transition pathways for other IT professionals are not well developed

New cyber security graduates are not the only possible supply of workers for the industry. There is a significant opportunity to adapt the skills of existing IT professionals to enable them to take up more specific cyber security roles. A breakdown of IT occupations that are most sought after by the cyber security industry, as detailed in Exhibit 37, reveals a large stock of IT workers with potentially transferable skills.[69]

For example, the five IT occupations most relevant to the cyber security industry boast a workforce of more than 225,000 people outside cyber security. They comprise of a range of specialists—from database and system administrators to computer network professionals and support technicians. Targeted training could enable these people to switch jobs and join the cyber security workforce.

Exhibit 37:



To be sure, skills shortages are found across the entire Australian ICT industry, and it is unrealistic to assume that the demand for cyber security specialists could be met just by re-training existing IT professionals.[70] Still, the cyber security industry with its high wages and strong growth outlook would likely be attractive for a significant number of IT workers wishing to accelerate their careers. The difficulty for many firms to find experienced cyber security staff and their willingness to pay wage premiums signal that too little has been done so far to help these workers transition.

Interviews with public officials, company executives and academics indicate that some government agencies and firms have drawn on the broader pool of general IT professionals to fill specialist cyber security roles. However, these skill transfers often occur without the necessary training, which impairs their effectiveness. Anecdotal evidence suggests that many organisations shy the expense or struggle to make training staff available to help workers from other industries or IT areas gain a foothold in the cyber security sector. A successful skills transfer is possible, though, as proven by some financial institutions in Australia that offer IT staff a six-months intensive 'apprenticeship' to help them transition into more specific cyber security roles.

Vocational training providers have an important role to play in facilitating the transition of workers by offering shorter, non-degree courses in cyber security. A number of institutions have already responded to the growing need for cyber security training by expanding their offerings. In Victoria, Chisholm TAFE and Box Hill Institute are both offering Certificate IV qualifications focused on cyber security, as is the ACT's Canberra Institute of Technology. TAFE SA, South Australia's largest vocational education and training provider, recently announced a partnership with a listed US cyber security provider to address the industry's skill shortage. It will offer new cyber security training courses under the umbrella program "Fortinet Network Security Academy" designed to "help fill the pipeline of cybersecurity experts needed to manage and thwart increasingly sophisticated cyberattacks".[71]

There are also a number of private sector training organisations, such as Ionize and UXC Saltbush, which both provide training for the Australian Signals Directorate's Information Security Registered Assessors Program. Overall, however, there is still plenty of scope for registered training organisations to become involved in cyber security.

Several steps could be undertaken to establish more visible and attractive pathways for the professional development of cyber security workers. Chapter 4.3 (*Make Australia the leading centre for cyber security education*) provides further detail on those recommended actions.

Australia has difficulties in retaining cyber talent

> **"Students with Distinction and high Distinction averages are receiving $100k job offers to leave in their second or third year and are not completing. Many of these graduates are leaving to take up positions in the [Silicon] Valley."**
>
> —Professor of cyber security at an Australian university

Interviews with a range of industry participants suggest that Australia is at risk of a 'brain drain' in the cyber security industry. Both company executives and university course coordinators have observed that recruiters are increasingly successful in luring Australia's top university talent abroad. Even before graduating, many students commit to taking up a role in Silicon Valley or elsewhere. In

interviews, some employers also expressed a reluctance to invest in staff training and development out of fear they could lose their highest-skilled workers to well-resourced U.S. competitors. Mobility of Australian workers into different markets can deepen their skills and experience, providing benefits from the Australian industry upon their return. However, some of these workers won't return and their departure does decrease the talent pool on offer for Australian cyber security firms. The supply of workers through the education system needs to take account of this loss to overseas.

Equally, there are signs that Australia could make better use of foreign professionals to reverse the 'brain drain'. While the number of Temporary Work (Skilled) visas (subclass 457) issued to workers classified as ICT Security Specialists—the largest occupational group within the cyber security industry—has steadily increased over the last decade, only 74 of these visas were granted in the fiscal year 2015-16.[72] Based on based for ANZSCO 262112 ICT Security Specialist, they are estimated to make up no more than two per cent of all ICT Security Specialists working in the Australian industry.

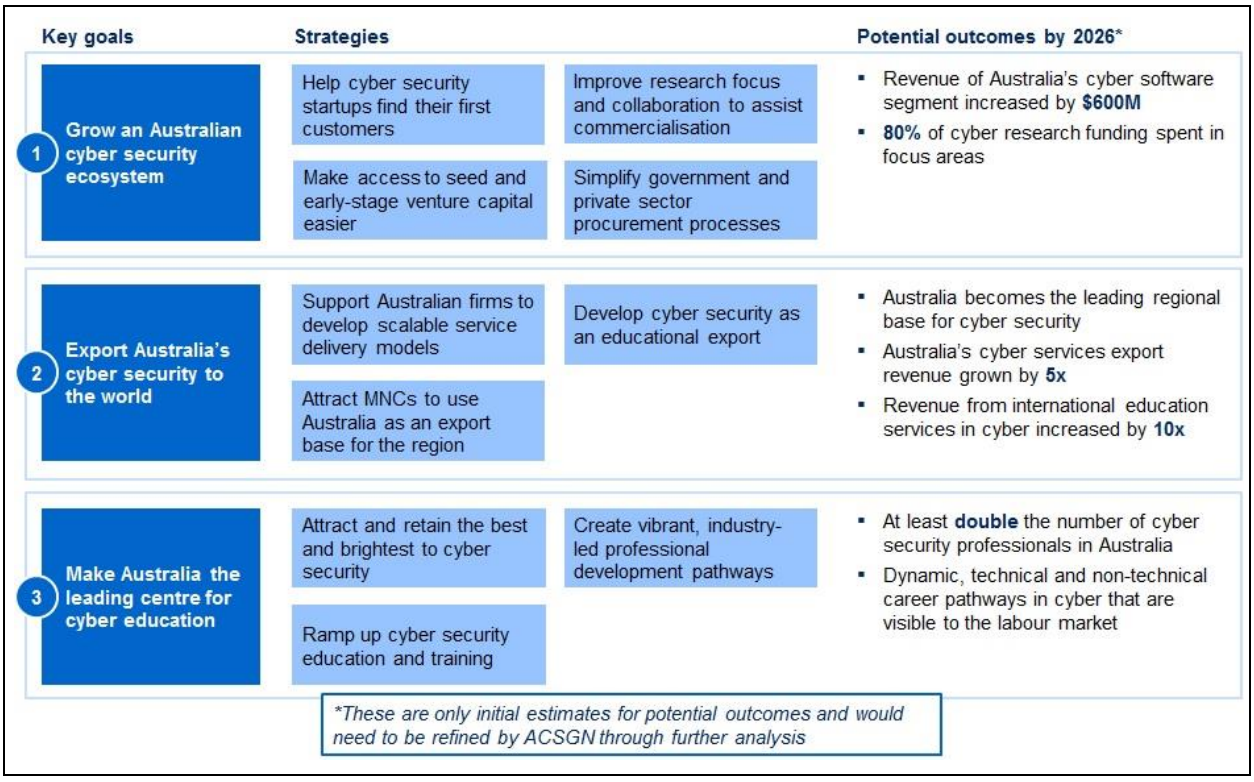
Chapter 4.3 (*Make Australia the leading centre for cyber security education*) lists a range of actions that could help Australia attract and retain the world's best and brightest cyber security talents, including scholarships with 'return of service' obligations and more efficient pathways for skilled migration to Australia for cyber security professionals.

4. Building a competitive Australian industry

While there is great potential for Australia to grow and succeed in the focus segments and the wider cyber security industry, the challenges are not insignificant and need to be properly addressed. Given the urgency of this opportunity and the eagerness of many other countries to also seize this moment in cyber security, that needs to happen fast. The Australian Government has already announced in its Cyber Security Strategy various measures that will help the Australian cyber security industry flourish, and many are already beginning to be implemented.

Based on the focus segments and the challenges, Australia should pursue three goals in order to develop a highly capable and globally competitive cyber security industry. Exhibit 38 explains these goals and the strategies that sit within them.

Exhibit 38:



4.1 Grow an Australian cyber security ecosystem

Australia's cyber security industry lacks the strong domestic ecosystem to compete effectively on a global scale. The local network of specialist firms, researchers, government bodies and training institutions that make up Australia's cyber security industry 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. If Australia wants to become a global market leader in cyber security and serve a substantial share of additional security demand over the next decade, it needs a stronger, more coherent cyber security ecosystem.

To achieve this, Australia will need 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 a greater collaboration between firms, 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 firm to sharpen its profile and refine its offering to be better aligned with global market needs, which increases business prospects.

Existing measures

The Australian government's National Innovation and Science Agenda comprises a suite of initiatives that back startups and entrepreneurs and their ability to generate economic growth and new jobs.[73]

The program includes a Business Research and Innovation Initiative, which provides funding for entrepreneurs to create new products and innovations that meet defined government needs, while retaining their intellectual property and the right to commercialise the ideas in Australia or overseas.[74]

In addition, the agenda vows to create more opportunities for startups to do business with government through the Digital Marketplace, an online platform connecting government agencies with firms offering digital services. The Marketplace has just opened for cyber security firms, which can now join other companies in competing for a share of the government's A$5 billion-a-year budget on external information and communication technology services.[75]

Various initiatives by Australian states and territories support the national efforts to improve the collaboration between government agencies and cyber security firms. For example, the government of New South Wales announced in its latest NSW Government ICT Strategy that it will try to use

smarter procurement processes when engaging with firms—from startups to global businesses—to grow the local digital economy.[76]

The Australian Government is also actively promoting the ingenuity of Australian cyber security firms abroad as part of its Landing Pads program, which aims at enabling startups to "rapidly fine-tune their pitch, commercialise their offering, identify partners, customers and investors, and access global markets".[77] A recent example includes a mission to San Francisco, where a delegation of senior Australian government officials and cyber security firms met with key US industry players and cyber security experts to explore business opportunities.[78]

Actions

	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, e.g. piloting, investment partnerships • Providing access to business coaching for startups • Undertaking showcases to promote Australian cyber security products and services to potential customers	ACSGN	Action
Recommendation that the Australian Government encourage industry investors in the CSIRO Innovation Fund to also become first customers for Australian cyber security start-ups that the Fund supports	Government	Explore
For startups and small organisations, to mature business operations and systems in order to work effectively with first customers	Industry	Action

Improve research focus and collaboration to assist commercialisation

Australia is home to several world-class universities and research institutions that are on the leading edge of cyber security innovation. Yet a diffuse funding system and weak links between academics and business limit the effectiveness of Australia's research capabilities.

The scattered approach to public R&D funding for cyber security in Australia should be replaced 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. ACSGN has developed Knowledge Priorities for cyber security in consultation with industry and researchers, located in Appendix A. The knowledge priorities will be

used to set out industry research needs and commercialisation opportunities for Australia's cyber security sector, as well as inform the activities of ACSGN as it works with stakeholders across the economy to improve the sector's research focus, collaboration and commercialisation outcomes. These 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.

Existing measures

The Australian government has already begun to strengthen the capabilities of Data61, which plays an important role in facilitating the collaboration between researchers and industry (see Box 7). Plans outlined in Australia's Cyber Security Strategy include the launch of a cyber-specific PhD scholarship program at the national science organisation CSIRO, which will allow students to work alongside Australia's leading data scientists at the interface between academia and the business world.[79]

There is also an existing proposal to pursue a scaled research program as well as consideration for the launch of a Cyber Security Innovation Lab that would bring together startups, researchers, entrepreneurs, multinational corporations and government officials to create and commercialise new ideas in cyber security.[80]

Actions

	Lead actor	Status
Identify areas of research strength that support the initial focus segments, based on Australia's existing research capabilities	ACSGN	Action
ACSGN to 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	ACSGN 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 network of researchers and organisational practitioners to better connect researchers with industry's future needs and identify emerging challenges and opportunities	ACSGN	Explore
Invest in the development of stronger collaboration capabilities, including offering work placements for postgraduate students	Industry	Action

Make access to seed and early-stage venture capital easier

Australian cyber security firms 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.

Existing measures

The Australian government already provides access to expert guidance and grants to help businesses commercialise their novel products, processes and services. The initiative, known as "Accelerating Commercialisation", is part of the Entrepreneurs' Programme.[81]

Further support for the commercialisation of early-stage innovation in Australia comes from a new program that is jointly funded by the national science agency CSIRO, the Australian government and private-sector companies. The "CSIRO Innovation Fund", launched in December 2016 and endowed with A$200 million, will invest in startups, spin-off companies and existing small firms to help Australia's home-grown innovations become successful businesses.[82]

The national Incubator Support initiative provides targeted funding to improve the prospects of Australian startups achieving commercial success in international markets. The initiative supports entrepreneurial activity and contributes to the development of Australia's innovation ecosystem.[83]

Last year, the Australian government also increased the incentive for investors to fund innovative companies at the early and growth stages of a startup. From 1 July 2016, anyone investing in "Early Stage Venture Capital Limited Partnerships" will enjoy additional tax offsets, a move designed to attract greater levels of international venture capital into Australia's most innovative industries. The government also has the Venture Capital Limited Partnerships programme, which aims to stimulate Australia's venture capital sector by attracting foreign investors and is also open to domestic investors.[84]

Actions

	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, eg international VC funds entering Australian market, better access to investments made by Australian superannuation and wealth funds	ACSGN	Action

Form an informal panel of CIOs and CISOs that can rapidly vet startups' products for VC investment	ACSGN	Explore
Develop the scale and maturity of incubators and accelerators that have a cyber focus	ACSGN	Action

Simplify government and private sector procurement processes

Many large companies and government agencies—both state and Federal—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 firms, which are often defeated by larger rivals with more experience, reputation and resources.

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 firms in the provision of cyber security products and services to government and big corporates.

Existing measures

The Australian government has begun to remove market entry hurdles for small firms through its "Digital Marketplace", an online platform for buyers and sellers of various ICT products and services. Recent changes aim to make it easier for small cyber security firms to work with government agencies.[85]

Actions

	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, e.g. introduction of maximum contract sizes • Working with state and Federal government agencies to identify opportunities for piloting of technologies offered by Australian firms	ACSGN	Action
Recommendation that the Australian Government partially subsidise the costs of Australian Government product certification (e.g., EPL) and service accreditation (e.g., IRAP) for Australian SMEs	Government	Explore
Innovate around procurement processes to identify requirements that can be relaxed for startups and SMEs	Industry	Action

4.2 Export Australia's cyber security to the world

Mounting cyber threats will propel 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 firms develop and maintain a strong export focus. If Australia wants to become a leading cyber security provider in the Asia-Pacific region, local firms 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 firms still lack the scale to effectively compete in markets outside Australia and contribute to global value chains. This is particularly evident for cyber security services firms, 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 indicate that 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 firms would deliver particularly strong economic gains.

Support Australian firms to develop more scalable business models

The key obstacle for many Australian cyber security firms, especially in services, is a lack of scalability in their business models. This means that 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 firms to improve the scalability of their businesses will be critical to export growth.

Existing measures

Cyber security firms wishing to expand into international markets can apply for financial assistance through the Australian government's Export Market Development Grants scheme. The scheme is designed to help small and medium-sized Australian businesses to develop export markets and promote their offerings abroad.[86]

The Australian Trade and Investment Commission (Austrade), the government's key trade promotion agency, also provides tailored business services to encourage Australian firms to become exporters. These services include help with understanding export markets, competitors, potential customers and available financial assistance.[87]

Australian state and territory governments offer additional assistance or funding to companies seeking help to start exporting.[88]

Actions

	Lead actor	Status
ACSGN to work with government(s) to deepen the understanding of export opportunities for Australian cyber security through a detailed market analysis	ACSGN with government agencies	Explore
Analyse the amenability of Australia's existing services strengths to remote delivery models (particularly in the protection stack)	ACSGN	Action
ACSGN to 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	ACSGN with government agencies	Explore
Identify ways to increase scale through partnerships and invest in the development of scalable, managed service models	Industry	Explore

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.[89] 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.

Existing measures

Austrade has already established a brand—Future Unlimited—for promoting Australian education internationally. Future Unlimited reassures students, and their parents, that their investment in an Australian education will be returned in the form of better career and life opportunities; it implies global career options; and reflects the idea of pathways and internationally recognised qualifications and skills.[90] The current branding strategy does not reference cyber security, however.

The Australian Government, in its Cyber Security Strategy, has also pledged to "build cyber capacity in the Indo-Pacific region and globally, including through public-private partnerships".[91]

Actions

	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	Explore
Recommendation that the Australian Government, working with the ACSGN, 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 (e.g., Future Unlimited)	Government with ACSGN	Explore

Attract MNCs to use Australia as an export base for the region

Most of Australia's cyber security needs are currently met by big multinational corporations (MNCs). They play an important role, not just as security providers, but also as employers. Yet 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 country's proximity to Asia and its potential to serve as a regional export base. Many foreign companies are already attracted to Australia because of its stable political environment, favourable business climate, and its diverse and well-educated workforce.

A range of incentives could be used to 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 firms 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.

Existing measures

All state and territory governments already offer a range of programs and investment promotion packages to attract foreign investors and businesses. The Australian Government also provides grants and other funding to businesses that need help to start exporting.[92]

Actions

	Lead actor	Status
Conduct detailed analysis of the existing export benefits of Australian operations of MNCs, and identify areas of comparative advantage for Australia as a cyber security export base for MNCs	ACSGN	Action
Work with State and Territory governments to develop investment attraction packages that meet the needs of MNCs with cyber security offerings and play to jurisdictional strengths in the diverse spread of cyber security capabilities	ACSGN	Explore

4.3 Make Australia the leading centre for cyber security education

Cyber security firms worldwide are struggling to expand their businesses, as they can't 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 firms 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, and while universities have begun to launch new study courses, they won't generate the graduate volume needed to keep pace with the industry's rapid expansion.

This skills shortage needs to be addressed quickly. It is already hindering the growth of the Australian cyber security industry. 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 firms 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 industry.

The responsibility doesn't lie solely with universities and other higher-education providers, but also with vocational training organisations and industry itself. Australian firms need to offer more, and better, opportunities for 'on-the-job' training of cyber security graduates. Meanwhile, more programs are needed that help equip professionals from various backgrounds with cyber security relevant skills, so they can transition into the industry.

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

are increasingly promoting 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 scope to better align Australia's immigration system with the strong demand for cyber security workers to make Australia more attractive as a workplace for international cyber security professionals.

Existing measures

LifeJourney, a US-based online education company with offices in Melbourne, has developed an internet platform to inspire students to pursue STEM careers. The initiative, Day of STEM, aims at promoting cyber security to high school students and is supported by a range of large technology companies and universities, including La Trobe University, Telstra, Westpac and Cisco Systems.[93]

The Australian government has committed in its latest Cyber Security Strategy to "continue to raise awareness in schools of the core skills needed for a career in cyber security".[94]

Actions

	Lead actor	Status
Recommendation that the ACSGN 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	ACSGN, government(s) and other relevant stakeholders	Explore
Increase the number of 'co-op' style scholarships for high-school students and consider 'return of service' obligations to encourage students to remain in Australia	Industry & training institutions	Explore
Introduce a voluntary 'Digital Nation' program, where post-secondary students gain work experience in digital professions including cyber security	ACSGN with industry	Explore
Provide efficient paths for immigration of skilled cyber security professionals by: • Recommending that the Australian Government include ICT Security Specialists to the Skilled Occupations List • Working with training institutions to structure education programs to meet the requirements of relevant visas	Government Training institutions	Explore Action

Ramp up cyber security education and training

Australia's education system is struggling to produce enough cyber security graduates to meet the current and future workforce demand. Labour market projections suggest that the total volume of Australian graduates that will emerge in coming years is insufficient to resolve the cyber security industry's skills shortage—even when accounting for several newly launched cyber security study courses at leading local universities. This means the output of cyber security education and training programs needs to be substantially increased to ensure Australia's cyber security industry can realise its full growth potential.

Businesses and education 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 UNSW, have emerged in recent years (see Box 11). They can serve as a blueprint for further collaborations to increase Australia's pool of cyber security workers with industry-relevant skills.

Existing measures

In its Cyber Security Strategy, the Australian government has acknowledged that developing highly-skilled cyber security professionals is an urgent need and announced the establishment of "academic centres of excellence" to enhance the quality of cyber security courses, teachers and professionals in Australia. The objective of these centres of cyber security excellence is also to "help inspire students to think about careers in cyber security and study STEM subjects at school".[95]

Actions

	Lead actor	Status
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 curricula • Supplementing teaching staff with industry personnel and exploring opportunities for this participation to be formally recognised in professional standards • Regularly revising curricula and course structure to maintain relevance	ACSGN Industry/Training institutions	Action

Ensure that senior executives, board directors and policymakers have access to high-quality cyber security training programs	ACSGN	Action

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 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 specialising in cyber security, and improving opportunities for on-the-job training, including graduate programs, which are currently limited to larger Australian firms.

Existing measures

The Australian government has committed A$1.9 million over the next four years through June 2020 "to address the nation's critical shortage of skilled cyber security professionals". The money will be used to create Academic Centres of Cyber Security Excellence (ACCSE) in several Australian universities. Key tasks of these new ACCSE are to encourage more young people to study cyber security and to increase the number of post-graduates with job-ready cyber security skills.[96]

A number of larger businesses, including Optus and Commonwealth Bank of Australia, have signed partnership agreements with Australian universities at the forefront of cyber security research to co-design and deliver courses, including short courses that could be part of transition pathways.

Actions

	Lead actor	Status
Expand the range of training/re-training and transition models available by: • Establishing an apprenticeship model for cyber security that will enable more hiring of graduates • Create industry-led rapid training/re-training courses to better enable transition to cyber security from other professions	ACSGN Industry	Action Action
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	Explore

4.4 Summary of strategies and actions

Captured below is a summary of the actions and recommendations identified above. For those identified for action/exploration by ACSGN, it will develop delivery mechanisms as it continues to evolve its program of work to grow Australia's cyber security industry and mature Australia's cyber security ecosystem. Recommendations identified for Australian governments are described for exploration and consideration, in partnership with the private sector and research community where possible and relevant to do so.

Grow an Australian cyber security ecosystem:

Key goals	Strategies	Actions	Lead actors	Status
1 Grow an Australian cyber security ecosystem	Help cyber startups to find their first customers	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, eg piloting, investment partnerships ■ Providing access to business coaching for startups ■ Undertaking showcases to promote Australian cyber security products and services to potential customers	ACSGN	Action
		Recommendation that the Australian Government encourage industry investors in the CSIRO Innovation Fund to also become first customers for Australian cyber security startups that the Fund supports	Government	Explore
		For startups and small organisations, to mature business operations and systems in order to work effectively with first customers	Industry	Action
	Improve research focus and collaboration to assist commercialisation	Identify areas of research strength that support the initial focus segments, based on Australia's existing research capabilities	ACSGN	Action
		ACSGN to 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	ACSGN 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 network of researchers and organisational practitioners to better connect researchers with industry's future needs and identify emerging challenges and opportunities	ACSGN	Explore
		Invest in the development of stronger collaboration capabilities, including offering work placements for postgraduate students	Industry	Action
	Make access to seed and early-stage venture capital easier	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, eg international VC funds entering Australian market, better access to investments made by Australian superannuation and wealth funds	ACSGN	Action
		Form an informal panel of CIOs and CISOs that can rapidly vet startups' products for VC investment	ACSGN	Explore
		Develop the scale and maturity of incubators and accelerators that have a cyber focus	ACSGN	Action
	Simplify government and private sector procurement processes	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, eg introduction of maximum contract sizes ■ Working with state and Federal government agencies to identify opportunities for piloting of technologies offered by Australian firms	ACSGN	Action
		Recommendation that the Australian Government partially subsidise the costs of Australian Government product certification (eg, EPL) and service accreditation (eg, IRAP) for Australian SMEs	Government	Explore
		Innovate around procurement processes to identify requirements that can be relaxed for startups and SMEs	Industry	Action

Key goals	Strategies	Actions	Lead actors	Status
2 Export Australia's cyber security to the world	Support Australian firms to develop more scalable business models	ACSGN to work with government(s) to deepen the understanding of export opportunities for Australian cyber security through a detailed market analysis	ACSGN with government agencies	Explore
		Analyse the amenability of Australia's existing services strengths to remote delivery models (particularly in the protection stack)	ACSGN	Action
		ACSGN to 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	ACSGN with government agencies	Explore
		Identify ways to increase scale through partnerships and invest in the development of scalable, managed service models	Industry	Explore
	Develop cyber security as an educational export	Establish marketing presence in cyber security in key target markets and develop partnerships with local industry that have training needs	Education and training institutions	Explore
		Recommendation that the Australian Government, working with ACSGN, 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 (eg, Future Unlimited)	Government with ACSGN	Explore
	Attract MNCs to use Australia as an export base for the region	Conduct detailed analysis of the existing export benefits of Australian operations of MNCs, and identify areas of comparative advantage for Australia as a cyber security export base for MNCs	ACSGN	Action
		Work with State and Territory governments to develop investment attraction packages that meet the needs of MNCs with cyber security offerings and play to jurisdictional strengths in the diverse spread of cyber security capabilities	ACSGN	Explore

Key goals	Strategies	Actions	Lead actors	Status
3 Make Australia the leading centre for cyber education	Attract the best and brightest to cyber security	Recommendation that the ACSGN 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	ACSGN, government(s) and other relevant stakeholders	Explore
		Increase the number of 'co-op' style scholarships for high-school students and consider 'return of service' obligations to encourage students to remain in Australia	Industry & training institutions	Explore
		Introduce a voluntary 'Digital Nation' program, where post-secondary students gain work experience in digital professions including cyber security	ACSGN with industry	Explore
		Provide efficient paths for immigration of skilled cyber security professionals by: ■ Recommending that the Australian Government include ICT Security Specialists to the Skilled Occupations List	Government	Explore
		■ Working with training institutions to structure education programs to meet the requirements of relevant visas	Training institutions	Action
	Ramp up cyber security education and training	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	ACSGN	Action
		■ Seeking opportunities to build significant industry experience component into curricula ■ Supplementing teaching staff with industry personnel and exploring opportunities for this participation to be formally recognised in professional standards ■ Regularly revising curricula and course structure to maintain relevance	Training institutions	Action
		Ensure that senior executives, board directors and policymakers have access to high-quality cyber security training programs	ACSGN	Action
	Create vibrant, industry-led professional development pathways	Expand the range of training/re-training and transition models available by: ■ Establishing an apprenticeship model for cyber security that will enable more hiring of graduates	ACSGN	Action
		■ Create industry-led rapid training/re-training courses to better enable transition to cyber security from other professions	Industry	Action
		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	Explore

5. The role of ACSGN

The Australian Cyber Security Growth Network was established to help the domestic cyber security industry grow and become more capable and competitive, and to establish Australia as a leading force in the rapidly expanding global cyber security market.

Developing a highly capable and globally competitive cyber security industry in Australia will deliver significant economic benefit. It must be led by industry itself, in partnership with the research and training institutions and government agencies that make up the cyber security ecosystem.

Specifically, the role of ACSGN is to act as a multiplier and connector for the Australian cyber security industry. What does that mean? Exhibit 39 outlines the key roles that ACSGN will play and the outcomes that are desired for each role.

To measure its impact in promoting the capabilities and competitiveness of the Australian cyber security industry, ACSGN will also develop a set of metrics that measure the change in desired outcomes over time.

It is important to clearly define the role of ACSGN to avoid duplication with the agenda of several other organisations and agencies that have been recently created or reshaped to support the industry as part of the Australian Government's Cyber Security Strategy. The strategies and actions outlined for ACSGN in this Plan have been carefully considered to complement various other existing plans and initiatives to strengthen the competitiveness of the Australian cyber security industry. ACSGN will continue to identify opportunities to work within the framework of existing plans and to improve the use of existing sources of government funding.

Exhibit 39:

As a multiplier, ACSGN will:	Desired outcomes
Work to develop the capabilities of Australian cyber security firms, particularly in business operations, so they can more effectively capture opportunities for growth and connect to global value chains.	■ Improved business operations capabilities of Australian cyber security firms ■ Greater participation by Australian cyber security firms in global value chains
Increase the return on our R&D investment by focusing our research efforts on areas of existing research capability that support the focus segments	■ Greater share of research investment—public and private—aligned with the knowledge priorities and needs of focus segments
Support strong demand for cyber security in Australia by ensuring policymakers and senior executives understand the capabilities of the Australian industry	■ Improved understanding of cyber security needs by Australian policymakers and senior executives
Improve the scalability and exportability of our cyber security firms by helping to identify and develop new business and delivery models, especially in services	■ Development of more scalable delivery models by Australian cyber security services firms ■ Increased number of services firms sustainably exporting

As a connector, ACSGN will:	Desired outcomes
Increase the quality and scale of interaction between industry and researchers in cyber security to ensure our growth is built on a platform of innovation through collaboration	■ Greater number of partnerships between industry and researchers in cyber security ■ Increased number of startup firms emerging from collaboration with research institutions
Improve the growth opportunities of Australian cyber security firms by connecting them with a wider range of funding pathways for commercialisation of innovation	■ Increased commercialisation funding accessed by Australian cyber security firms
Connect Australian cyber security firms with potential customers in both the public and private sectors, and help address barriers that prevent our firms from competing effectively for work	■ Greater number of private and public sector organisations acting as anchor customers for Australian cyber security firms

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 industry. They will be used to inform the activities of the ACSGN 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. ACSGN 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.

The 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*.[97]

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 pro-active 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

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 IoT, 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

To estimate industry revenue and revenue growth by segment and the share of demand currently met by Australia firms, a proprietary model was built based on a range of data sources, including Gartner and IDC. ((Footnote 98: Market size by country obtained from Gartner (2016), *Information Security, Worldwide, 2014-2020, 3Q16 Update*; software market share data obtained from IDC (via custom data requests).)) The assumptions for market share and export share for Australian firms are shown in Exhibit A1, as well as the source of those assumptions.

Exhibit A1:

Market share assumptions

Share of Australian market by type of firm
% of Australian cyber security spend

			Source/rationale
Hardware	Domestic players	5%	Estimate based on conversations with IDC, and analysis of domestic market share by provider
	Foreign players with core business in Australia	0%	Core business (i.e. design) is typically kept in the home jurisdiction
	Foreign players with sales team only	65%	Foreign product firms in Australia typically have a sales team only
	Foreign players with no presence	30%	Interview with IDC (70% of firms serving Australian customers have an Australian office)
Software	Domestic players	5%	Estimate based on conversations with IDC, and analysis of domestic market share by provider
	Foreign players with core business in Australia	0%	Core business (i.e. software development) is typically kept in the home jurisdiction
	Foreign players with sales team only	65%	Foreign product firms in Australia typically have a sales team only
	Foreign players with no presence	30%	Interview with IDC (70% of firms serving Australian customers have an Australian office)
Services	Domestic players	20%	Team judgment, based on evidence from interviews (international services players receive much more attention)
	Foreign players with core business in Australia	50%	
	Foreign players with sales team only	25%	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%	Assumed to be low as it is difficult to provide services with no in-country presence

Export assumptions

Exports as a % of revenue by type of firm
% of firm revenue

			Source/rationale
Hardware Software	Domestic players[1]	66%	Interviews with industry players combined with team judgment
Services	Domestic players	10%	Interviews with stakeholders, which suggest few services firms are currently exporting from Australia
	Foreign players with core business in Australia	10%	

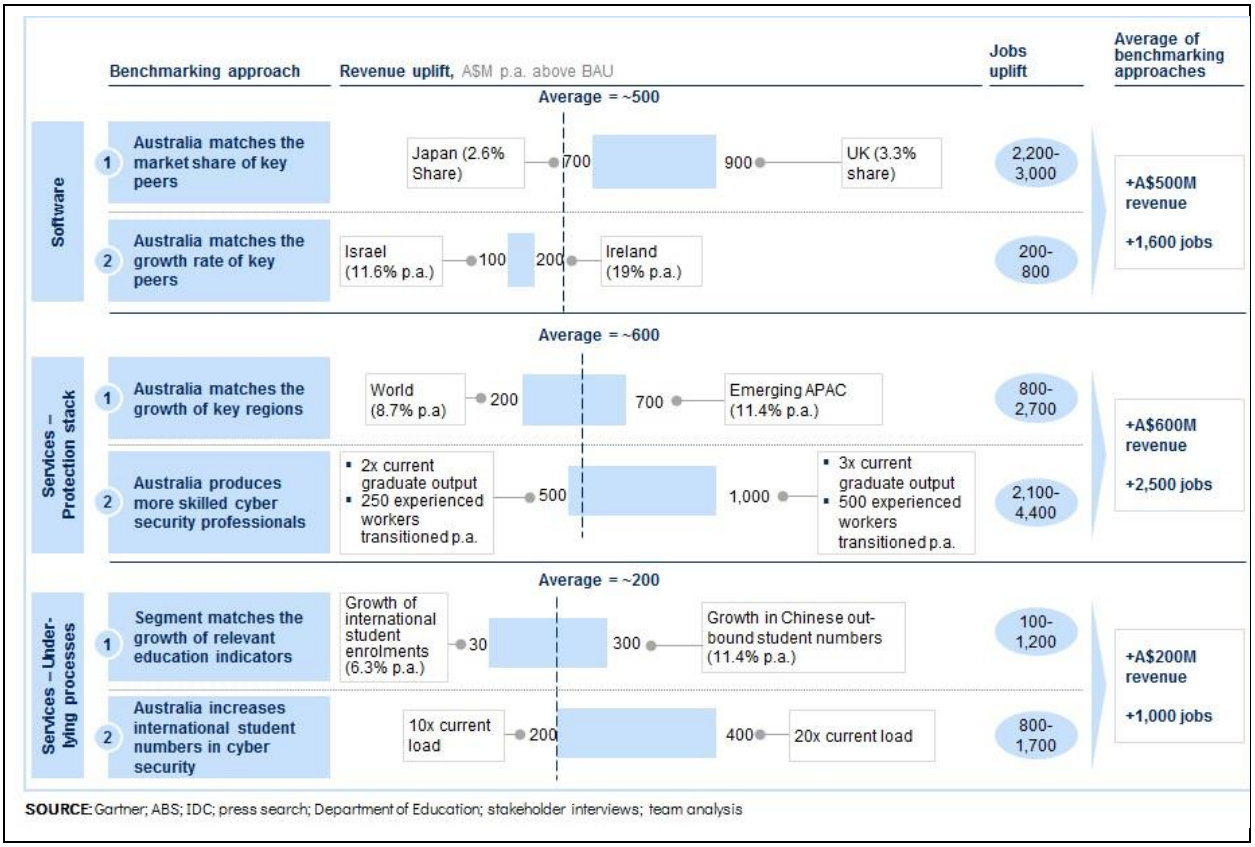
1 Export assumptions were not required for "foreign players with core business in Australia" as this group was assigned a zero market share for software and hardware.

SOURCE: Expert & stakeholder interviews, UN World Input-Output tables, team analysis

The size of the prize

The size of the prize was calculated by averaging the potential uplift in performance of each of the three initial focus segments from two different methodologies. Details of this approach are outlined in Exhibit A2.

Exhibit A2:



[1] 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 report focuses primarily on external spending, it proposes several actions (e.g. skills development) that would strengthen both outsourced cyber providers and in-house cyber security teams.
[2] IBM Corp. (2016), *Cyber Security Intelligence Index*. Available at: http://www-03.ibm.com/security/data-breach/cyber-security-index.html
[3] Symantec Corp. (2016), *Internet Security Threat Report*. Available at: https://www.symantec.com/security-center/threat-report
[4] Australian Cyber Security Centre (2016), *Threat Report*, page 14. Available at: https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf and Australian Cyber Security Centre (2015), *Threat Report*, page 7. Available at: https://www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf
[5] Australian Government (2016), *Australia's Cyber Security Strategy*. Available at: https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf
[6] Telstra (2017), *Cyber Security Report*. Available at: https://www.telstra.com.au/content/dam/tcom/business-enterprise/campaigns/pdf/cyber-security-whitepaper.pdf
[7] Australian Prudential Regulation Authority (2016), *Information Paper: 2015/16 Cyber Security Survey Results*. Available at: http://www.apra.gov.au/AboutAPRA/Documents/Information-Paper-Cyber-Security-2016-v4.pdf
[8] This Sector Competitiveness Plan is primarily focussed on the delivery of cyber security products and services to organisations. Individuals do purchase cyber security products, but they account for less than six per cent of global demand. Gartner (2016), *Information Security, Worldwide, 2014-2020, 3Q16 Update*
[9] Full title: Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.
[10] ICD (2016), *Worldwide Security Spending Guide 1H 2016 Update*.
[11] Security management, assessment and analytics is a sub-segment of security operations. The market size of security operations services overall is US$25.0 billion.
[12] 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/
[13] 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
[14] Australian dollar figures are converted from US dollar-denominated market data using the 2016 average exchange rate of US$0.74.
[15] Gartner (2016), "Gartner says IT spending in Australia to reach almost A$85 billion in 2017 as the battle for the digital platform begins". Available at: http://www.gartner.com/newsroom/id/3490317
[16] Australian Cyber Security Centre (2015), *Cyber Security Survey: Major Australian Businesses*. Available at: https://www.acsc.gov.au/publications/ACSC_CERT_Cyber_Security_Survey_2015.pdf
[17] Services are more likely to be provided locally due to the lower exportability of cyber security services compared to hardware and software.
[18] Austrade (2016), "Australia's export performance in 2015". Available at: http://www.austrade.gov.au/news/economic-analysis/australias-export-performance-in-2015
[19] National Fintech Cyber Security Hub (2017), "Overview". Available at: https://www.fintechcyberhub.com/
[20] World Bank (2017), *World Development Indicators*. Available at: http://data.worldbank.org/indicator/NY.GDP.TOTL.RT.ZS
[21] Austrade (2016), "Australia's export performance in 2015". Available at: http://www.austrade.gov.au/news/economic-analysis/australias-export-performance-in-2015
[22] AlphaBeta/McKinsey (2017), "Survey of Australian CIO and CISO purchasing factors".

[23] Amitai Ziv, Haaretz (2015), "Israel emerges as global cyber superpower". Available at: http://www.haaretz.com/israel-news/business/.premium-1.658076
[24] 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
[25] Singapore Government (2017), *National Cybersecurity R&D Programme*. Available at: https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme
[26] Australian Government (2016), *Cyber Security - Capability Statement*. Available at: http://science.gov.au/scienceGov/ScienceAndResearchPriorities/Pages/Cybersecurity.aspx
[27] ARC (2016), "Grants Dataset". Available: http://www.arc.gov.au/grants-dataset
[28] Australian Government Business (2017), "Accelerating Commercialisation funding offers". Available at: https://www.business.gov.au/Assistance/Accelerating-Commercialisation/Accelerating-Commercialisation-funding-offers
[29] Innovation and Science Australia (2016), *Performance Review of the Australian Innovation, Science and Research System*. Available at: https://industry.gov.au/Innovation-and-Science-Australia/Documents/ISA-system-review/Performance-Review-of-the-Australian-Innovation-Science-and-Research-System-ISA.pdf
[30] Innovation and Science Australia (2016).
[31] Referenced in Australian Government (2016), *Cyber Security - Capability Statement*. Available at: http://science.gov.au/scienceGov/ScienceAndResearchPriorities/Pages/Cybersecurity.aspx
[32] 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
[33] Global Risk Institute (2016), "A quantum of prevention for our cyber-security". Available at: http://globalriskinstitute.org/publications/quantum-computing-cybersecurity/
[34] 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
[35] 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
[36] 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
[37] QuintessenceLabs (2017), "QuintessenceLabs Sees Additional Investment from Westpac Group to Strengthen Partnership". Available at: http://www.quintessencelabs.com/about-us/newsroom/press-releases/quintessencelabs-additional-investment-westpac-group-cybersecurity/
[38] 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
[39] Australia Research Council (2017), *Grants Dataset*. Available at: http://www.arc.gov.au/grants-dataset
[40] Australian Government, Office of the Chief Economist (2016), *Australian Innovation System Report*. Available at: https://industry.gov.au/Office-of-the-Chief-Economist/Publications/Documents/Australian-Innovation-System/2016-AIS-Report.pdf
[41] 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
[42] 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

[43] 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/

[44] 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

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

[46] Australian Cyber Security Research Institute website, available at: https://www.acsri.org.au/about-acsri/

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

[48] Stone & Chalk (2016), "Submission to the Inquiry into Australia's Future in Research and Innovation".

[49] CIO (2016), "Dimension Data and Deakin University join forces in Cyber Security Incubator". Available at: http://www.cio.com.au/mediareleases/28010/dimension-data-and-deakin-university-join-forces/

[50] AlphaBeta/McKinsey (2017), Survey of Australian CIOs, CISOs and Cyber Security Companies

[51] World Economic Forum (2017), *The Global Competitiveness Report 2016-17*. Available at: http://reports.weforum.org/global-competitiveness-index/

[52] Australian Government, Innovation and Science Australia (2016), *Performance Review of the Australian Innovation, Science and Research System 2016*. Available at: https://industry.gov.au/Innovation-and-Science-Australia/Documents/ISA-system-review/Performance-Review-of-the-Australian-Innovation-Science-and-Research-System-ISA.pdf

[53] AlphaBeta/McKinsey (2017), "Survey of Australian CIO and CISO purchasing factors".

[54] PwC/ICF GHK/Ecorys (2014), SMEs' access to public procurement markets and aggregation of demand in the EU. Available at: http://ec.europa.eu/internal_market/publicprocurement/docs/modernising_rules/smes-access-and-aggregation-of-demand_en.pdf

[55] https://www.tenders.gov.au/?event=public.son.view&SONUUID=9EF01E95-D79C-2555-7DB88D34335030ED

[56] For a detailed list of criteria see: https://marketplace.service.gov.au/assessment-criteria#cyber

[57] NSW Government Department of Finance, Services & 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

[58] AISA (2016), The Australian Cyber Security Skills Shortage Study. Available at: https://www.aisa.org.au/Public/Training_Pages/Research/AISA%20Cyber%20security%20skills%20shortage%20research.aspx

[59] CSIS & Intel Security (2016), "Hacking the Skills Shortage". Available at: https://www.mcafee.com/ca/resources/reports/rp-hacking-skills-shortage.pdf

[60] Burning Glass (2016), Job Market Intelligence: Cybersecurity Jobs, 2015. Available at: http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf

[61] We estimate that 1,800 workers will retire and another 2,000 will move overseas over the next 10 years. However, the loss of workers to industry rivals in the U.S. and elsewhere is difficult to quantify and could surpass our estimates.

[62] Department of Education and Training (2016), "uCube – Higher Education Data Cube". Available at: http://highereducationstatistics.education.gov.au/

[63] La Trobe University (2016), "Optus & La Trobe tech-collaboration". Available at: http://www.latrobe.edu.au/news/articles/2016/release/optus-And-la-trobe-tech-collaboration

[64] Macquarie University (2016), "$10 million partnership with Optus for new cyber security hub". Available at: http://www.mq.edu.au/thisweek/2016/05/30/10-million-partnership-optus-new-cyber-security-hub/#.WMXn1_l9600

[65] 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/
[66] Commonwealth Bank of Australia (2015), "Commonwealth Bank and UNSW confront chronic cyber security shortage". Available at: https://www.commbank.com.au/about-us/news/media-releases/2015/commonwealth-bank-and-unsw-confront-chronic-cyber-security-shortage.html
[67] Commonwealth Bank of Australia (2016), "Commbank Cyber Prize 2016". Available at: https://www.commbank.com.au/guidance/newsroom/commbank-cyber-prize-2016-201612.html
[68] CSIS & Intel Security (2016), "Hacking the Skills Shortage". Available at: https://www.mcafee.com/ca/resources/reports/rp-hacking-skills-shortage.pdf
[69] Note: These IT occupations are most frequently listed in job advertisements for cyber security roles.
[70] The most commonly mentioned occupations recruitment agencies have difficulty filling are SAP developers, cyber security specialists, SCCM deployment, mobile developers, and Sharepoint specialists. See: https://docs.employment.gov.au/system/files/doc/other/ausitprofessions_1.pdf
[71] TAFE SA (2017), "TAFE SA launches first Fortinet Network Security Academy in Asia Pacific region". Available at: https://www.tafesa.edu.au/tafe-sa-news/2017/02/28/tafe-sa-launches-first-fortinet-network-security-academy-in-asia-pacific-region
[72] Australian Department of Immigration and Border Protection (2016), "Subclass 457 visas granted pivot table". Available at: https://www.border.gov.au/ReportsandPublications/Documents/statistics/457-quarterly-report-30-09-2016.pdf.
[73] Australian Government (2017), "Startups and entrepreneurs". Available at: http://www.innovation.gov.au/audience/startups-and-entrepreneurs
[74] Australian Government (2017), "Business Research and Innovation Initiative". Available at: http://www.innovation.gov.au/page/business-research-and-innovation-initiative
[75] Australian Government (2017), "Digital Marketplace". Available at: http://www.innovation.gov.au/page/digital-marketplace and https://www.dta.gov.au/news/marketplace-expansion/
[76] NSW Government (2016), Digital + 2016. NSW Government ICT Strategy Final Update. Available at: https://www.finance.nsw.gov.au/ict/sites/default/files/resources/Digital_Strategy_2016_20151125.pdf
[77] Australian Government (2017), "About Landing Pads". Available at: http://www.australiaunlimited.com/LandingPads/about-landing-pads
[78] Austrade (2016), "US cyber security mission to showcase Australian credentials". Available at: http://www.austrade.gov.au/news/latest-from-austrade/2016/us-cyber-security-mission-to-showcase-australian-credentials
[79] Australian Government (2016), *Australia's Cyber Security Strategy*, p.8
[80] Data61/KPMG/Stone & Chalk/Australia-Israel Chamber of Commerce (2016), *Startup secrets: How Australia can create new businesses with fintech and cyber security industry collaboration*
[81] For more details see here: https://www.business.gov.au/assistance/accelerating-commercialisation
[82] Australian Government (2016), "CSIRO Innovation Fund to commercialise early stage innovations". Available at: http://www.innovation.gov.au/page/csiro-innovation-fund
[83] Australian Government (2016), "Incubator support initiative". Available at: http://www.innovation.gov.au/page/incubator-support-programme
[84] Australian Government (2016), "Changes to Venture Capital Limited Partnerships". Available at: http://www.innovation.gov.au/page/changes-venture-capital-limited-partnerships and "Venture Capital Limited Partnerships". Available at https://www.business.gov.au/assistance/venture-capital-limited-partnerships
[85] Australian Government (2017), "Digital Marketplace"
[86] Australian Trade and Investment Commission (2017), "Export Market Development Grants". Available at: http://www.austrade.gov.au/Australian/Export/Export-Grants/What-is-EMDG

[87] Australian Trade and Investment Commission (2017), "Expand your business by exporting". Available at: http://www.austrade.gov.au/Australian/export
[88] For an overview see here: http://www.austrade.gov.au/Australian/How-Austrade-can-help/other-assistance
[89] 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
[90] Austrade (2011), "Future Unlimited". Available at: https://www.austrade.gov.au/Australian/Education/Future-Unlimited
[91] Australian Government (2016), *Australia's Cyber Security Strategy*, p. 63.
[92] Austrade (2017), "Guide to Investing". Available at: http://www.austrade.gov.au/International/Invest/Guide-to-investing/Australian-Government-support-programs/Assistance-exporting-from-Australia
[93] Government (2017), "Live a life in the day of a STEM leader". Available at: http://www.science.gov.au/scienceGov/news/Pages/Live-a-life-in-the-day-of-a-STEM-leader-17-November-2015.aspx
[94] Australian Government (2016), *Australia's Cyber Security Strategy*, p. 65.
[95] Australian Government (2016), *Australia's Cyber Security Strategy*, p. 54.
[96] Australian Government Department of Education and Training (2017), "Academic Centres of Cyber Security Excellence". Available at: https://www.education.gov.au/academic-centres-cyber-security-excellence-accse
[97] 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)