Australian Government
Department of Industry, Science,
Energy and Resources
Industry Growth Centres

AustCyber
Australian Cyber Security Growth Network

AUSTRALIA'S CYBER SECURITY SECTOR COMPETITIVENESS PLAN

2020 UPDATE

Driving growth and global competitiveness

PLAN AT A GLANCE

2020 OVERVIEW

At least **US$147 billion** was spent on direct cyber security products and services globally in the last year

The gross value added of Australia's cyber security sector is approximately **A$2.3 billion**

26,500 workers are employed in cyber security in Australia

43% of cyber security businesses are exporting globally

There are now at least **350** sovereign cyber security providers in Australia

Australians spent approximately **A$5.6 billion** on cyber security from local and international providers in the last year

Australian cyber security providers generated **A$3.6 billion** in revenue – **A$3 billion** from the domestic market and **A$600 million** from international markets

Most of the businesses in Australia's cyber security sector are young – **40%** are under five years old and **66%** are less than ten years old

Collaboration in the sector is very high – **33–44%** of startups partner on product and service delivery solutions

Like most businesses, cyber security providers are having to change how they operate – **51%** report this as an effect of COVID-19

OUTLOOK FOR 2024

A$1.4 billion
in additional revenue generated by the Australian sector

7,000 additional jobs
added to Australia's economy, totalling 33,500 in the workforce

$7.6 billion
spent on cyber security in Australia from local and international providers

GROWTH CHALLENGES

1. **Market access barriers** – procurement processes make it harder for the local sector to access customers
2. **Innovation maturity** – many younger cyber providers struggle to access finance and skills to commercialise their solutions
3. **Export presence** – Australian cyber providers are not yet tapping the full potential of regional export markets
4. **Skills shortages** – while the skills pipeline has grown rapidly, maintaining momentum is critical

“Cyber security has emerged as one of Australia’s most promising growth sectors

ACTIONS FOR SUSTAINED GROWTH

1. Support Australia's digitising economy

- Ensure that Australia's digital growth is secure by design and in application, supporting productivity and trust across the economy
- Improve protection of industries that are rapidly digitising such as healthcare and manufacturing
- Support the Australian Government's cyber security agenda and encourage direct engagement with sovereign cyber capabilities by governments and industries

2. Capture global export opportunities

- Build upon existing relationships with export markets in the US and UK
- Expand Australia's presence into high-potential markets in Asia
- Be ready to take advantage of opportunities in Europe

3. Incentivise innovation and capital flows

- Focus effort on cyber security research hubs to concentrate R&D strength
- Grow and mature Australia's cyber security innovation infrastructure
- Promote increased investment from the right sources at the right time to better support cyber security company growth

4. Improve market maturity and access

- Support businesses in the sector to mature and scale
- Ensure government and large corporate procurement promotes market access
- Provide a supportive regulatory environment that builds and retains resilience and trust

5. Develop the skills of the future workforce

- Ensure growth in the nation's cyber security skill pipeline is maintained
- Lift cyber literacy of leaders and decision makers across governments and private sectors, regardless of organisational size or value chain positioning
- Transform Australia's cyber security workforce to capture benefits of diversity and inclusion

FOREWORD

The Australian cyber security sector is coming into its own. It is well positioned to enable the uptake and application of trusted digital technologies and practices in the global economy's recovery from the COVID-19 pandemic.

Cyber security continues to be one of the most rapidly expanding sectors worldwide, with global spending on cyber security products and services increasing by 30 per cent from 2017 to 2020. This year alone, Australians spent approximately A$5.6 billion on cyber security from both local and international providers, a figure that is expected to increase to A$7.6 billion by 2024.

While the pandemic is having economic impact on Australia's cyber security providers, it has accelerated digitisation trends and driven unprecedented domestic demand for cyber security. Trust in digital infrastructures and the data they carry is the mainstay of recovery from the pandemic – but also the means to drive productivity and effective diversification of the economy's base. This is reflected in a range of industries that have not traditionally been recognised as digitised industries, and are now seeking robust cyber-physical protection.

Over the next decade, the Australian cyber security sector will become larger, more diverse and more sophisticated. Providers will continue to refine their market offerings to meet their customers' varying cyber security needs and continue to support our changing economy. There will be new opportunities fuelling further growth as the application of technologies at the points of convergence between, and within, sectors create more complexity and pressure on systems and networks.

There are now over 500 providers in the domestic sector, supported by 26,500 workers employed in full time cyber security roles. At least 350 providers in the sector are considered sovereign. A closer look at the sector reveals it is characterised by new, innovative small and medium-sized enterprises (SMEs), with 88 per cent of providers having fewer than 100 employees.

This 2020 update to Australia's Cyber Security Sector Competitiveness Plan (SCP) draws on extensive industry consultation and research to provide a fresh picture of the global outlook, challenges, opportunities and priority actions needed to grow a vibrant and globally competitive cyber security sector that enhances Australia's future economic growth.

Last year's deep dive explored the underlying structural challenges of not yet having robust measurement of the sector's development. This year, through market and administrative data, as well as insights from AustCyber's inaugural sector-wide Digital Census, we have produced the first comprehensive measurement of the Australian cyber security sector – including state-by-state analysis. Consequently, figures in this SCP may be different or higher than estimated in previous SCPs as they are based on new and updated sources of data.

These fresh insights have allowed us to uncover the current state of the sector, outline the potential for the next growth phase and describe how to accelerate the momentum the sector has developed over the past five years.

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

The past year has seen progress in several areas and Australia is in a strong position. Cyber security is a foundational enabler of digitisation – it builds digital trust and gives businesses and consumers the confidence to transact online, adopt new technologies, and create new markets and commercial opportunities.

Reflecting this, it was a logical next step for us to add 'Australia's Digital Trust Report 2020' as a companion document to the SCP, joining the 'Australian Cyber Security Industry Roadmap' and 'CISO Lens Benchmark' as the premier suite of knowledge guiding sector growth and the economy's understanding of cyber security.

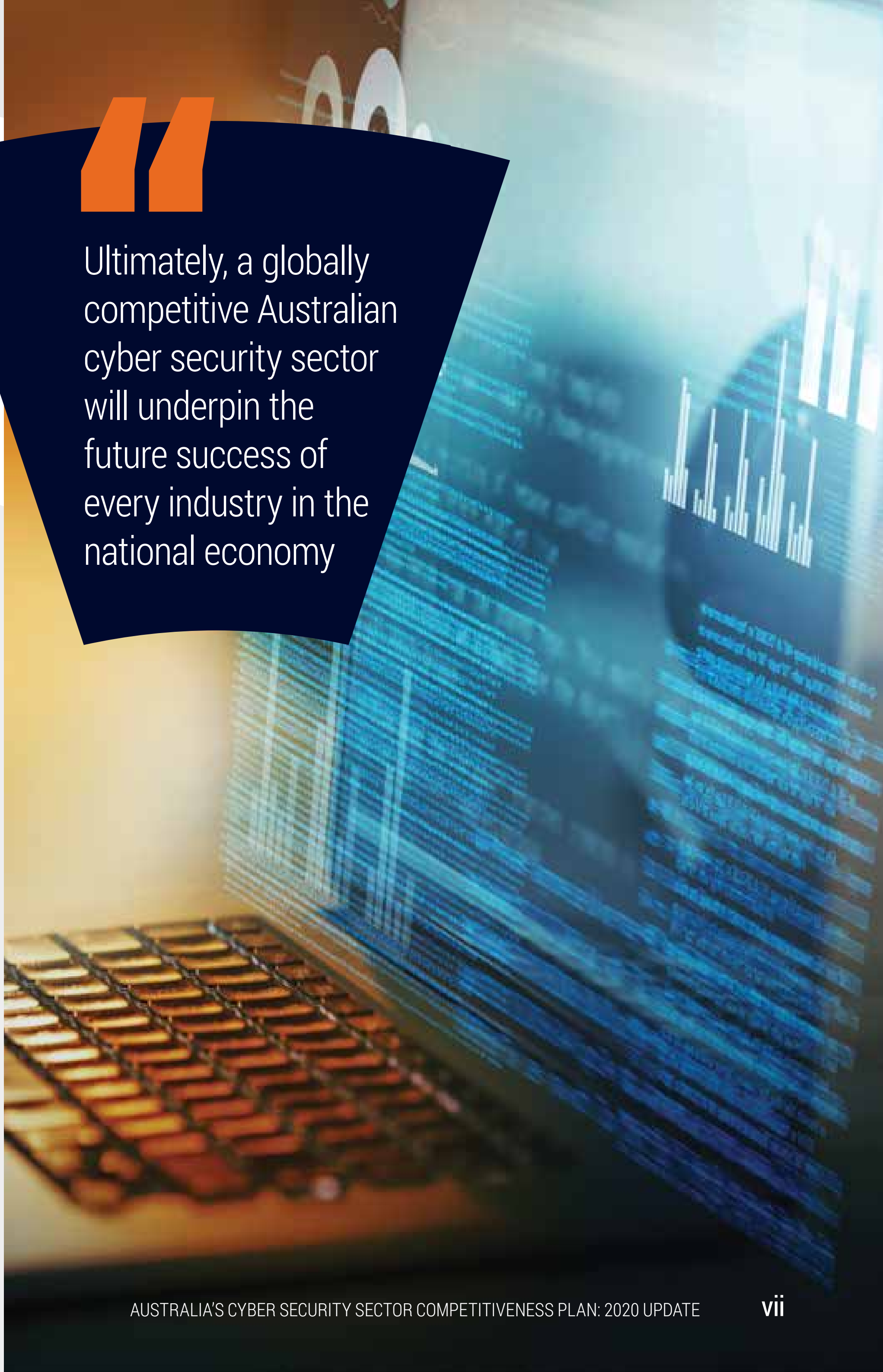
'Australia's Digital Trust Report 2020' highlights the role digital trust plays in attracting investment and driving jobs growth. It draws on data modelled by Synergy's Advanced Modelling Group to quantify the value of digital activity to the Australian economy and the impact of a significant cyber security incident.

While we are well placed for further growth and success as the sector continues to tackle familiar challenges relating to innovation, market maturity, investment and skills, more needs to be done to ramp up the momentum over the next 12 months and slowing down is not an option.

Governments, cyber security sector leaders, educators and investors all have crucial roles to play as the sector matures. Already, a host of effective sector development activities and initiatives have yielded success. The innovation environment continues to mature, more customers are looking to Australian providers, and a sophisticated skills training architecture has been developed.

Ultimately, a globally competitive Australian cyber security sector will underpin the future success of every industry in the national economy. Let's build on successes so far to foster innovation and generate increased investment and jobs through the creation and commercialisation of cyber security products and services.

Michelle Price
Chief Executive Officer, AustCyber



> Ultimately, a globally competitive Australian cyber security sector will underpin the future success of every industry in the national economy

WEBSITE
SEO
SOCIAL NETWORK
WEBSITE
VDO
MOBILE
WEBSITE
SEO
SOCIAL NETWORK
MOBILE
WEBSITE
VDO

CONTENTS

EXECUTIVE SUMMARY

The cyber security sector is flourishing in Australia: growth is strong, a vibrant cohort of young cyber security technology and service providers has emerged and the workforce is expanding.

Australia's cyber security sector is growing rapidly. Between 2017 and 2020, sector revenue has grown by A$800 million to A$3.6 billion across approximately 350 technology and service providers, who are supported by about 26,500 workers.

The average cyber security provider is young, small and active across the country. On average, they are 8.5 years old, and about 40 per cent are younger than five years. Their youth means that most of these providers employ relatively fewer workers: 88 per cent have fewer than 100 employees.

The COVID-19 pandemic has had short- and long-term economic effects on Australia's cyber security providers.

A few months after the start of the pandemic, surveys showed that, on average, providers with fewer than 20 employees had experienced a decline in revenue, while the revenue of larger providers was steady or had grown since it began.

Significantly, the pandemic has accelerated digitisation trends, which in turn drives demand for cyber security solutions and skills. It has also revealed the extent to which our national wellbeing relies on a range of industries that have not traditionally been recognised as digitised industries that require robust protection.

Australia's economy is digitising and the cyber security sector must be capable of meeting its protection needs.

Digitisation drives productivity gains and is at the centre of Australia's future economic prospects. Cyber security is a foundational enabler of digitisation: it builds digital trust and gives businesses and consumers the confidence to transact online, adopt new technologies and create new markets and commercial opportunities. This is apparent in a few recent examples such as the widespread adoption of cloud services and remote working tools and the ubiquity of e-commerce in modern retail trade. The next wave of technologies, such as the Internet of Things (IoT), sophisticated remote operations technology, quantum and artificial intelligence (AI), will further transform the economy.

The Australian cyber security sector will need to continue to mature and develop to secure increasingly complex digital value chains. This does not mean that only local suppliers should provide comprehensive protection to Australian businesses. Rather, our cyber security sector should be capable of coordinating and adapting a range of solutions from around the world to meet national needs.

Australia's cyber security sector should also become a global leader in the utlisation of secure by design principles, where the application of security guides the development of new digital technology and the rollout of new value chains. Australia is well placed to do this, especially in industries where we have competitive strategic advantage.

The sector is well placed for further growth and success as it continues to tackle familiar challenges relating to innovation, market maturity, investment and skills.

The maturity and competitiveness of the Australian cyber security sector is vital for future Australian prosperity. To achieve this, familiar challenges need to be addressed. New providers with quality offerings need to be supported, funded, connected to the market, and supplied with the skilled workers they need to succeed.

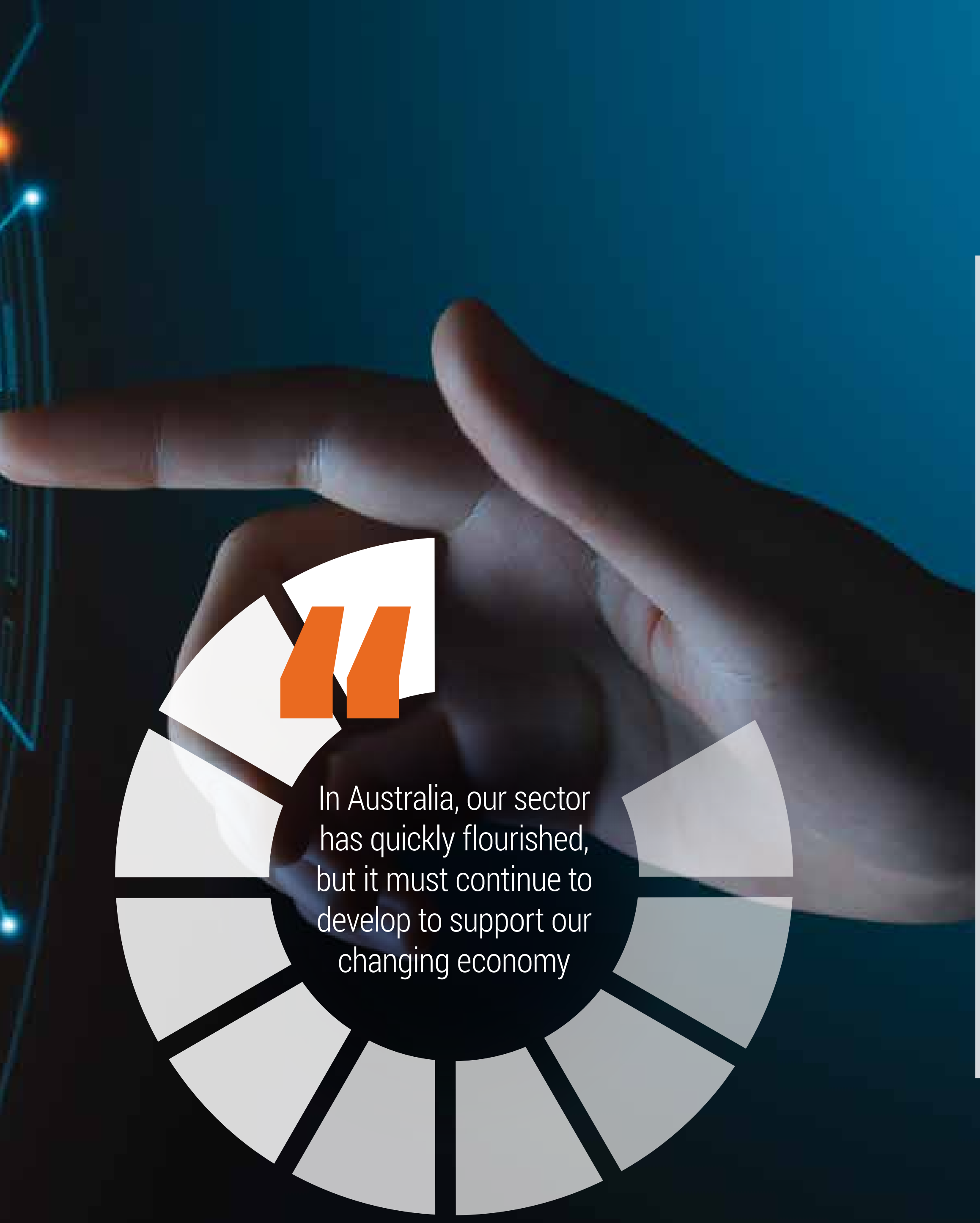
Governments, cyber security sector leaders, educators and investors all have crucial roles to play as the sector matures. Already, a host of effective sector development activities and initiatives have yielded success, including regulatory reform emerging from the Australian Government's Cyber Security Strategy 2020. The result is that Australia's cyber security innovation environment continues to mature, more customers are looking to buy from Australian cyber security providers, and a sophisticated skills training architecture has been developed.

Acknowledgements

In 2020, AustCyber conducted a sector-wide Digital Census of Australia's cyber security sector. The responses captured by this survey have enabled AustCyber to present more detailed insights into the sector than ever before. This Update has also been informed by extensive consultation with governments, the private sector and the research community in Australia and internationally. AustCyber gratefully acknowledges and thanks all who contributed, including:

- AARNet
- Accenture
- Amazon
- AUCloud
- Austrade
- BHP
- Bugcrowd
- CISO Lens
- Cyber Aware
- CyberCX
- CyCube
- Cynch Security
- CyRise
- Deloitte Australia
- Department of Home Affairs
- Dtex Systems
- EY Australia
- Government of South Australia
- IAG
- IBM Australia
- Penten
- PwC Australia
- Splunk
- Telstra
- Trustwave
- University of Queensland
- Westpac

AustCyber also acknowledges Bugcrowd, Cloud one – Conformity, CyberCX, Cydarm Technologies, Cynch Security, Detexian, elttam, FifthDomain, Kasada, truuth, Penten, Retrospect Labs, Secure Code Warrior and the University of Adelaide for their contributions to the case studies.



> In Australia, our sector has quickly flourished, but it must continue to develop to support our changing economy

In a digitising economy, cyber security is an essential economic enabler that mitigates threats and builds trust

The new economy is a digital economy. As we enter the third decade of the 21st century, digital technology is expanding beyond a handful of industries and becoming central to the whole economy. Digitisation brings a host of benefits: improved productivity, access to more markets, and the development of new products that solve old problems, to name just a few. But as digital tools proliferate, they offer more targets for malicious actors who have increasingly powerful and lucrative techniques.

Malicious cyber activity ranges from straightforward online fraud – such as scams using email, websites or chat rooms – to sophisticated cyber espionage and even catastrophic disruption of vital infrastructure, such as phone lines or power grids. Cybercrime doesn't just harm an organisation's business and reputation, it can also compromise a nation's security, stability and prosperity. The number of incidents of cybercrime has spiked in recent years, as perpetrators aggressively exploit flaws in digital infrastructure.

Cyber security, and its relationship with privacy and safety, is therefore a front-of-mind concern for business leaders, regulators and politicians who are anxious to shore up defences against adversaries who are devising new ways to exploit vulnerable systems and networks. The growing security needs of organisations are expected to underpin the rapid evolution of the global cyber security sector. Between 2017 and 2020, global spending on cyber security grew from US$113 billion to US$147 billion.

Source: Gartner (2020), *Forecast: Information Security and Risk Management, Worldwide, 2018–2024, 2Q20 Update*. Available at: https://www.gartner.com/en/documents/3988093/forecast-information-security-and-risk-management-worldw

1

THE AUSTRALIAN CYBER SECURITY SECTOR TODAY

Australia's cyber security sector has rapidly grown in response to strong demand for its critical services

Australia's cyber security sector has come a long way in a short time

Using data from AustCyber's Digital Census 2020, this chapter paints the most comprehensive picture yet of Australia's cyber security sector. Demand is growing, with Australians spending approximately $5.6 billion on cyber security in 2020 – from both local and international providers – a figure that is expected to increase to $7.6 billion by 2024. The local sector's revenue has grown by $800 million since 2017, to reach an estimated $3.6 billion this year. SMEs generate about a quarter of the cyber sector's revenue in Australia, with the rest directed to diversified professional services providers, technology integrators, mid-tier providers and defence contractors. Gross value added (GVA) of the Australian sector has been estimated for the first time in this report at $2.3 billion.

The sector is made up of young cyber security providers, and a workforce that's steadily growing

There are more Australian cyber security providers and workers than ever before. In 2020, approximately 350 providers make up the domestic sector. Among this group of young companies – the average age is 8.5 years and more than 40 per cent were founded in the past five years – there are success stories of companies that have flourished, becoming internationally recognised names.

The workforce has grown by 4,000 since 2016, reaching approximately 26,500 people who work for providers or staff internal security teams as businesses and government improve their cyber capabilities.

A closer look at the sector reveals that it is characterised by new, innovative SMEs, with more than 88 per cent of providers having fewer than 100 employees. SMEs and larger providers specialising in systems security account for the biggest portion of Australia's cyber security market. Many of their customers are government or defence organisations.

States and territories are developing their own communities to foster innovation

The sector is building its network across Australia, with clusters of innovation developing in major cities. AustCyber's National Network of Nodes will accelerate cyber capability development and innovation. Having a presence in states and territories will help to sharpen customer awareness of domestic cyber security capability and attract top talent.

Initially, the impact of COVID-19 appears to have hit micro and small providers hardest, while medium-sized companies have recorded an uptick in demand as customers adapt to digital modes of working and develop go-to-market strategies. Despite the short-term disruption to some service delivery, the pandemic is likely to accelerate the long-term transformation of the economy through technology and increased demand for cyber security.

[1] Gartner (2020), *Forecast: Information Security and Risk Management, Worldwide, 2018–2024, 2Q20 Update.* Available at: https://www.gartner.com/en/documents/3988093/forecast-information-security-and-risk-management-worldw

Australia spent approximately $5.6 billion on cyber security in 2020, with demand expected to reach $7.6 billion by 2024

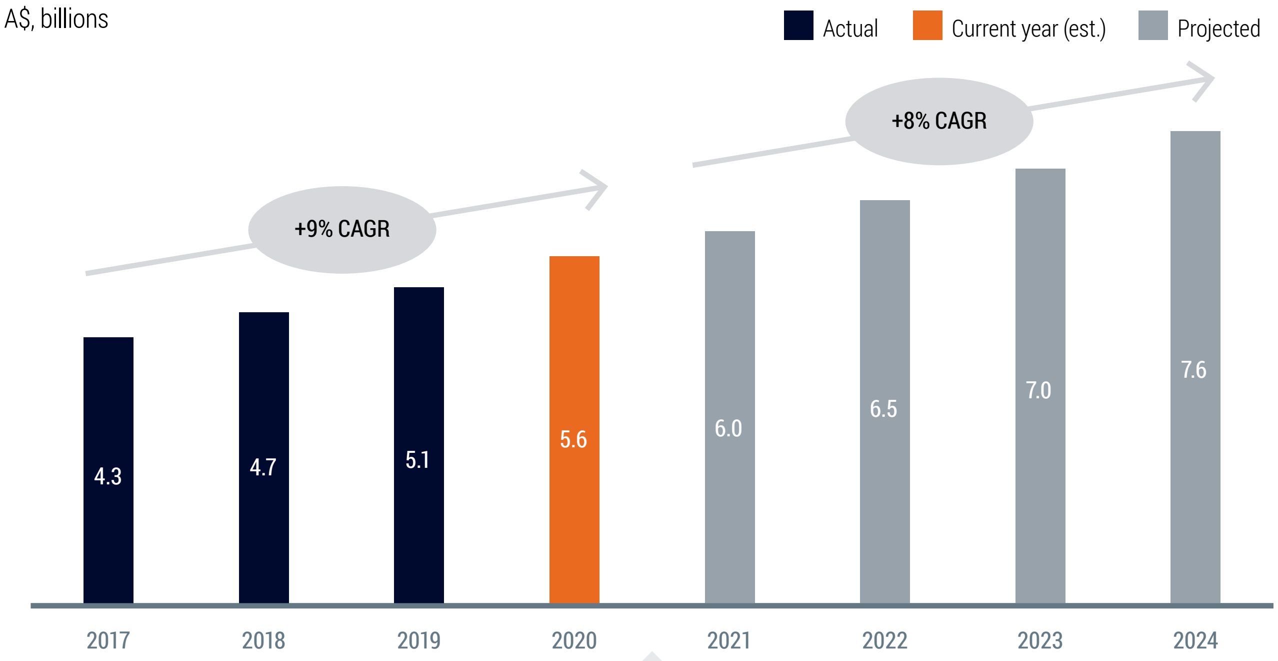
Demand for cyber security is rapidly growing, with spending increasing by nine per cent each year over the past four years.

There are several core drivers of demand. First, digitisation exposes businesses to more threats. Second, the overall threat environment is increasing, with several high-profile attacks – such as against NSW Government agencies, Toll Group and PayID – over the past year. Third, governments and regulators are requiring stronger security for critical infrastructure and systems of national significance.

Analysis based on available market data and expert interviews suggests that Australian demand will continue to grow by eight per cent per year, reaching as high as $7.6 billion by 2024. This is a slight reduction on previous growth of nine per cent, reflecting some slowness in the market as a result of the economic conditions caused by the COVID-19 pandemic. But the growth rate is still robust, considering the broader economic recession. The impact of COVID-19 is further explored on page 24. Globally, it is expected that spending on cyber security will reach US$207 billion by 2024.[1]

Figure 1

Australia's cyber security spend, 2017–24



97 per cent of Australia's total spend on cyber security comes from businesses, with consumer spending accounting for the remaining three per cent.

Note: The spending figures for 2017–24 are higher than estimated in previous SCPs. The higher figures are based on new sources of insight and updated data. The methodology is explained in the appendix.
Sources: Gartner, IBISWorld, AustCyber's Digital Census 2020, AlphaBeta analysis

[1] Gartner (2020), *Forecast: Information Security and Risk Management, Worldwide, 2018–2024, 2Q20 Update.* Available at: https://www.gartner.com/en/documents/3988093/forecast-information-security-and-risk-management-worldw

Growth in spending is reflected in the local sector's revenue, which has risen by $800 million since 2017

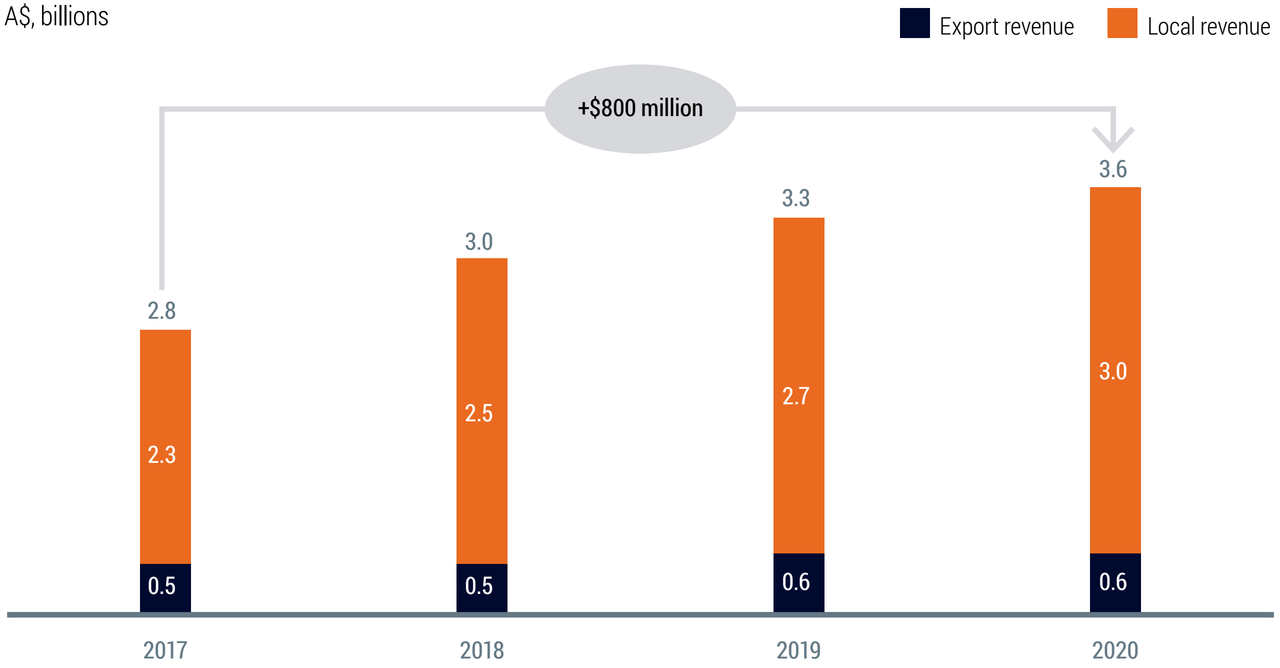
Australian cyber security revenue has grown substantially over the past four years. Between 2017 and 2020, sector revenue grew by $800 million – from $2.8 billion to $3.6 billion.

These gains have been made very quickly. Sector revenue grew by an average of eight per cent each year between 2017 and 2020. By contrast, the information, media and telecommunications (IMT) sector's revenue grew by just three per cent each year over the same period.[1] Australia's cyber sector revenue growth is increasing at a similar pace to overall spending on cyber security, indicating that the share of imports in the Australian market is relatively stable.

As the cyber threat landscape continues to evolve, sector revenue is forecast to continue to grow at about nine per cent each year over the next four years. The sector could reach $5 billion in revenue by 2024, which is nearly double its 2017 level.

Figure 2

Australia's cyber security sector revenue, 2017–20



Note: Australia's 2020 cyber security sector revenue figures and revenue growth figures are estimated using global spend data as at July 2020.
Sources: Gartner, IBISWorld, Austcyber's Digital Census 2020, AlphaBeta analysis

Note: Australia's cyber security sector includes all cyber security activity that occurs in Australia, where the economic value is added in Australia, including by foreign-owned entities. IMT's growth rate for 2020 was estimated using historical data.

[1] Australian Bureau of Statistics (2020), *Australian Industry 2018–19*, Table 1, key data by industry subdivision. Available at: https://www.abs.gov.au/statistics/industry/industry-overview/australian-industry/latest-release

CASE STUDY

Startup success reflects sector's rapid growth

Australia is home to some of the world's fastest growing cyber security providers, many of whom have raised significant amounts of investment while expanding their operations globally.

bugcrowd

Bugcrowd is a crowdsourced security as a service provider, offering penetration testing, bug bounty programs and vulnerability disclosure to customers across a wide range of industries.

The company was founded in Australia in 2012, but moved their headquarters to San Francisco for better access to venture capital, shorter time-to-market and improved network effects.

Bugcrowd has raised over US$80 million in funding and investors include Paladin Capital Group, Blackbird Ventures, Rally Ventures, Costanoa Ventures, SalesForce Ventures, Triangle Peak Partners and First State Super. The company employs over 300 staff across their Australian, US and UK offices.

SECURE CODE WARRIOR

Founded in 2015, Secure Code Warrior enables developers to build secure code rather than having to review or retrofit security during or after development. The company also provides gamified developer training and can auto correct code security errors as code is being written.

SCW has raised over US$48 million in funding and investors include Paladin Capital, AirTree, Goldman Sachs, ForgePoint Capital and CISCO Investments. The company employs over 150 staff across their Australian, US, UK, Belgium and Iceland offices.

kasada

Kasada safeguards consumers and businesses from malicious online bots. Their solution protects businesses from automated attacks, botnets and targeted fraud – across web, mobile and API channels. Besides boosting online security, the company increases traffic visibility and improves customer experience.

Kasada is one of Australia's fastest growing cyber security startups, reporting 500% revenue growth in 2019. Founded in 2015, Kasada has raised over US$20 million and investors include CSIRO's Main Sequence Ventures, Westpac's VC fund Reinventure Group, In-Q-Tel, TenEleven Ventures, Our Innovation Fund and former Australian Prime Minister Malcolm Turnbull.

Kasada is expanding its global footprint servicing customers in the ASX 100, Forbes Global 2000 and mid-sized enterprises in the US and UK.

TREND MICRO™ | Cloud One™ Conformity

Cloud One – Conformity works with organisations around the world to implement and maintain best-in-class infrastructure security, compliance and optimisation on the public cloud. Their solution helps businesses who rely on AWS, Azure and Google Cloud to ensure their information and data remains secure.

Cloud One – Conformity provides an example of a successful exit. Founded in 2016, it was acquired in 2019 for US$70 million by global security vendor Trend Micro. Cloud One – Conformity now has offices in Australia, US, UK and Canada.

SME providers received about a quarter of sector revenue in Australia

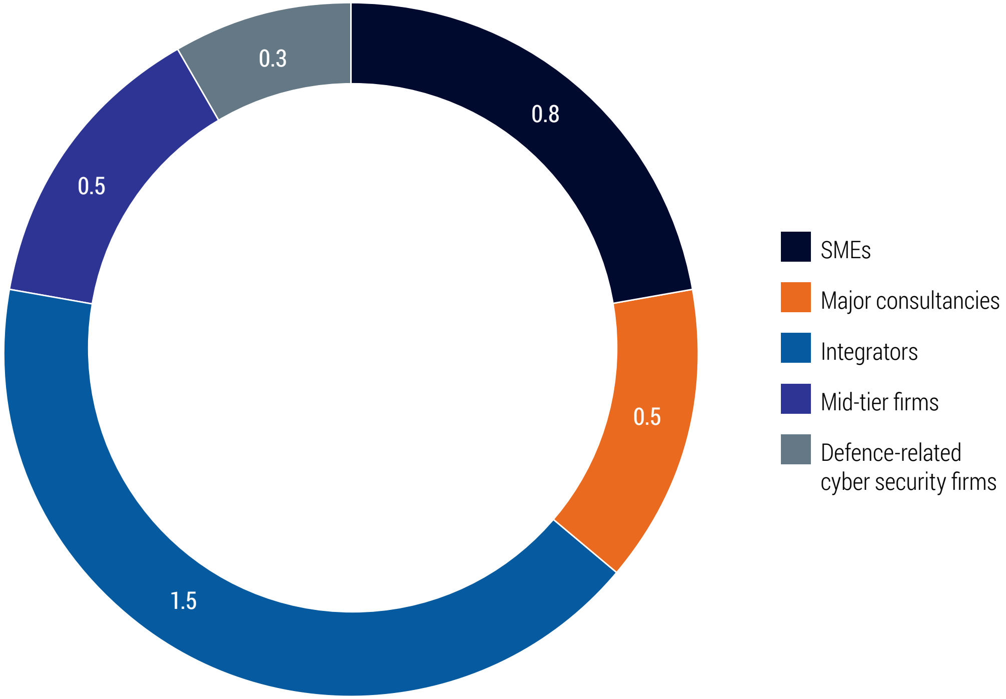
Australian cyber security providers are generating $3 billion in revenue from the domestic market and $600 million from international markets, totalling $3.6 billion.[1] Based on expert interviews, the Australian cyber security sector is segmented into five key groups:

- **SMEs:** startups and smaller providers. SMEs received approximately $800 million in revenue, which is around one-quarter of the sector's total revenue.
- **Major consultancies:** cyber security practices at major consulting firms. They are estimated to earn approximately $500 million in revenue.
- **Technology integrators:** large international diversified technology businesses that integrate systems and security. Integrators are capturing the largest share of the market, valued at an estimated $1.5 billion.[2]
- **Mid-tier firms:** scaled pure-play providers such as CyberCX, Tesserent and Trustwave. They account for an estimated $500 million of revenue.[2]
- **Defence-related firms:** providers focused on defence and national security, such as the so-called Defence Primes.[2]

Figure 3

Australia's cyber security sector revenue by provider segment

A$, billions; 2020 estimate



Survey question: What was the total revenue for your organisation in the 2019–20 financial year?
Sources: AustCyber's Digital Census 2020, customised data from illion

Australia's cyber security sector includes all cyber security activity that occurs in Australia, where the economic value is added in Australia, including by foreign-owned entities.

[1] Market data from Gartner and IBISWorld, supplemented with expert interviews

[2] Expert interviews and customised data from illion

The cyber security workforce has grown by 4,000 over the past three years

The substantial growth in cyber security spending in Australia has led to the workforce expanding by about 4,000 since 2017. A total of about 26,500 people work in the Australian cyber security sector today.

This estimate includes both employees in the cyber security sector and those in related roles, such as members of in-house cyber security teams and Chief Information Security Officers in other sectors.

Growth in jobs in cyber security has far outpaced the national average. Between 2017 and 2020, employment in the sector grew by six per cent each year, while the nation's overall workforce expanded by just two per cent each year.[1]

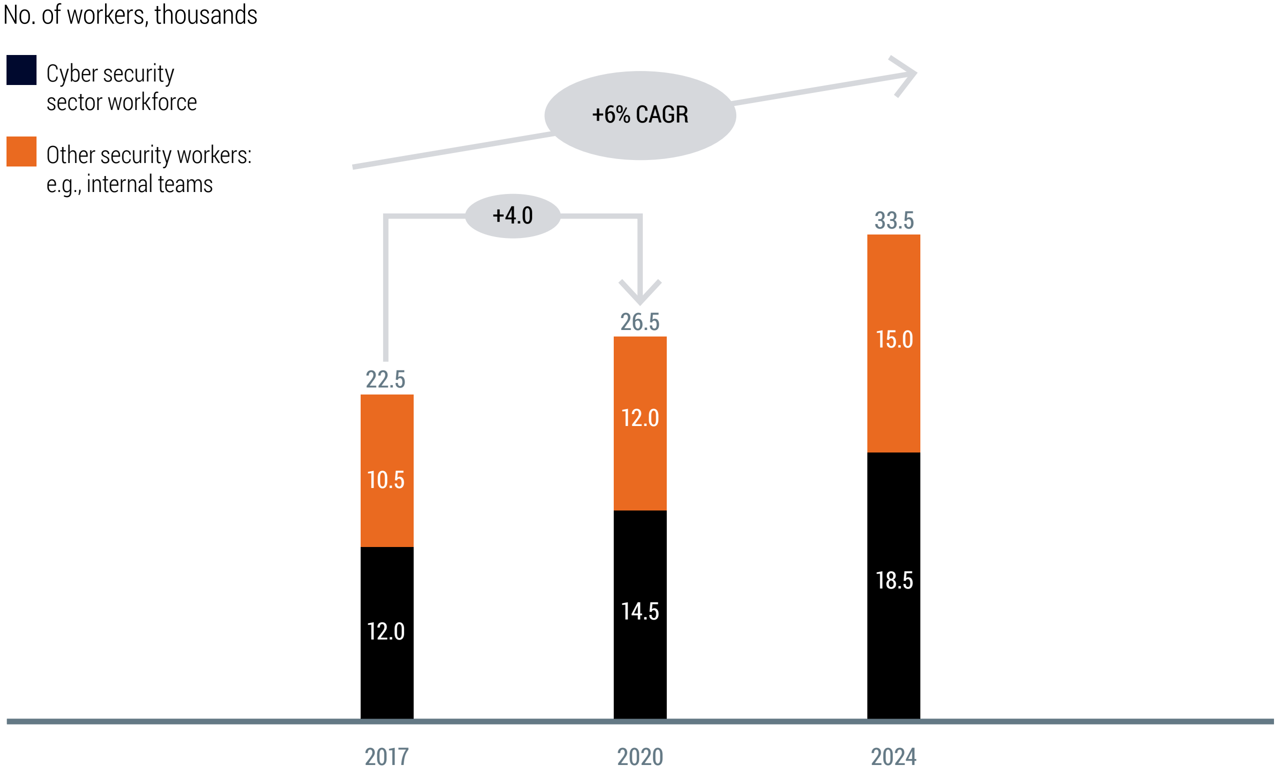
In absolute terms, the total number of **direct** jobs in the sector is comparatively small compared to other, more established industries. However, cyber security underpins the digitisation and growth of the entire economy, meaning it has a much greater impact on Australia's overall employment through **indirect** jobs.

Strong job creation in cyber security is likely to continue, with 7,000 more jobs expected to be added to Australia's economy by 2024.

A number of government and industry programs, such as the Australian Signals Directorate's CyberEXP Program and the Australian Defence Force's Cyber Gap Program, are focused on developing Australia's workforce to meet this growing demand. Further programs will be added into the economy in the next year as a result of the Australian Government's Cyber Security Strategy 2020 and initiatives of state and territory governments.

Figure 4

Australian cyber security workforce 2017–24



Note: The employment figures for 2017–24 are higher than estimated in previous SCPs. The higher figures are based on new and updated sources of data that were available for this SCP.

Sources: Gartner, IBISWorld, Australian Bureau of Statistics, Cyberseek Australia, AlphaBeta analysis

[1] Australian Bureau of Statistics (2020), *Labour Force, Australia, Detailed Quarterly.* Available at: https://www.abs.gov.au/statistics/labour/employment-and-unemployment/labour-force-australia-detailed-quarterly/latest-release

1 THE AUSTRALIAN CYBER SECURITY SECTOR TODAY

> AustCyber's Digital Census enables the calculation of GVA for the sector for the first time

For the first time, the gross value added of Australia's cyber security sector can be estimated, at $2.3 billion

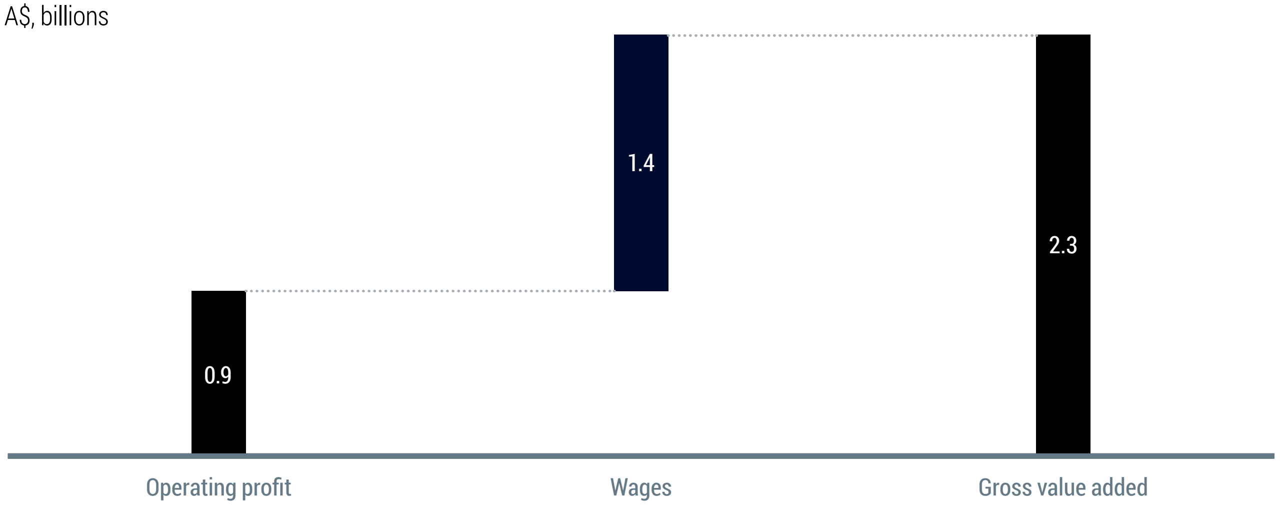
GVA (gross value added) is a measure of economic activity and can be used to estimate the contribution of the cyber security sector.

AustCyber's Digital Census enables the calculation of GVA for the sector for the first time. GVA is the sum of the profits and wages from economic activity in the sector. In 2020, the former is estimated at $900 million (25 per cent of revenue) and the latter at $1.4 billion, resulting in GVA of $2.3 billion. The sector's GVA is already comparable to other digital sectors such as computer software ($4.2 billion) and retail e-commerce ($3.2 billion).[1]

While GVA estimates the direct contribution of cyber security to the economy, it does not account for its role in enabling economic activity in other sectors. For example, the GVA of sectors such as banking and telecommunications would not be possible without robust cyber security. As our corporations, educational institutions and essential services become increasingly digitised, their success and impact largely rely on having trusted infrastructure and data.[2] The sector's role in a rapidly digitising economy is further explored in Chapter 2.

Figure 5

Estimated gross value added of Australia's cyber security sector, 2020



Profit	+	Wages	=	GVA (direct)
Profit estimate is based on data from more than 100 respondents to the Digital Census, scaled to account for sector size, as well as ABS data and public company reports		Total sector wages was estimated by applying a weighted average wages-to-revenue ratio from the Digital Census to total sector revenue, as well as ABS data		GVA was estimated by summing operating profits and wages. This estimate does not include indirect economic impacts

Note: Australia's 2020 cyber security sector revenue figures and revenue growth figures are estimated using global spend data as at July 2020.
Sources: Gartner, IBISWorld, AustCyber's Digital Census 2020, AlphaBeta analysis

Note: This is an experimental first pass calculation of GVA for Australia's cyber sector using Digital Census data, as well as ABS and publicly available data. As more robust data on the cyber sector becomes available, this measurement can be further refined. Retail e-commerce is estimated using Australian online retail sales' share of total Australian retail turnover.

[1] Australian Bureau of Statistics (2019), *Measuring digital activities in the Australian economy.* Available at: https://www.abs.gov.au/websitedbs/D3310114.nsf/home/ABS+Chief+Economist+-+Full+Paper+of+Measuring+Digital+Activities+in+the+Australian+Economy

[2] AustCyber (2020), *Australia's Digital Trust Report 2020.* Available at: https://www.austcyber.com/resource/digitaltrustreport2020

Most of the businesses in Australia's cyber security sector are very young, with more than 40 per cent of providers around or under five years old, and 66 per cent less than ten years old

Despite this, a number of younger Australian cyber security firms have found early success in both Australia and abroad. One example is ASX-listed Tesserent, which was founded in 2016 and specialises in managed security and security consulting. Over the past two years, it has acquired smaller cyber security providers such as Rivium, Pure Security and Seer Security, further adding to its suite of capabilities.

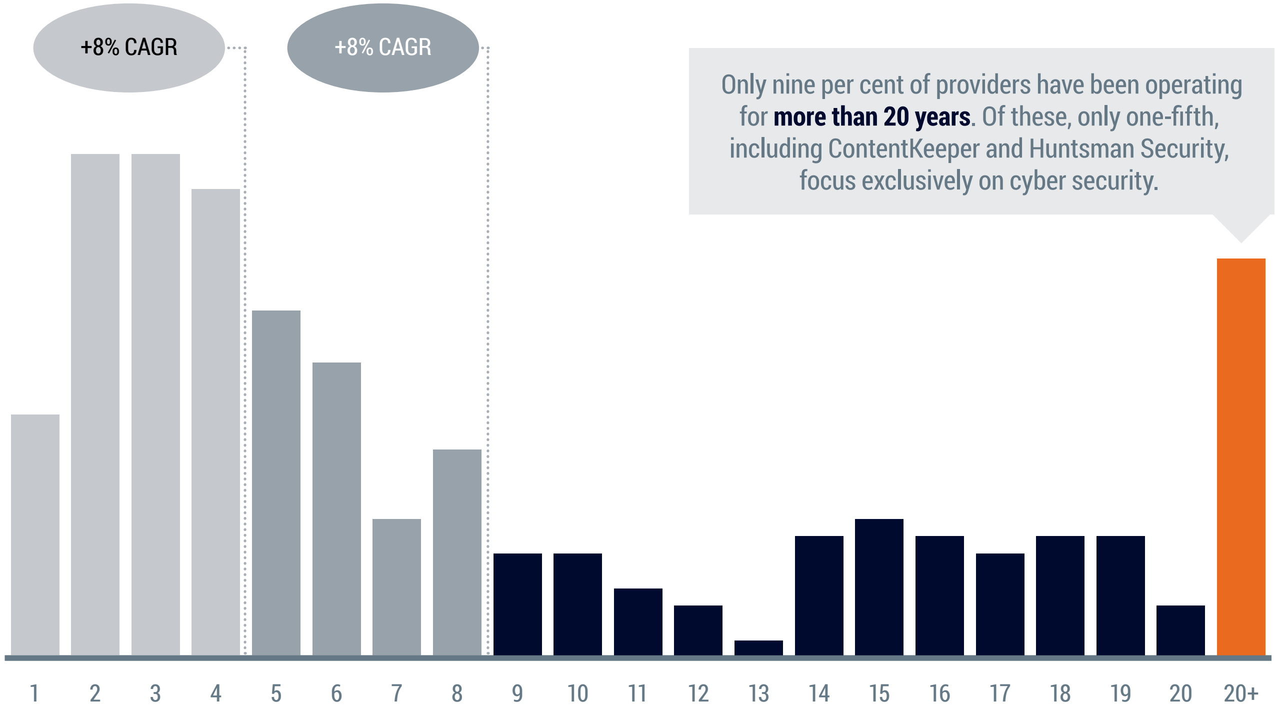
The average age of Australian cyber security providers is 8.5 years, and only nine per cent in the sector have been operating for more than 20 years.[1] Of the firms that are older than 20 years, only 23 per cent are dedicated cyber security providers.[2] The majority of these are services or IT businesses that offer cyber security as one part of their business.

The sector's youth opens up many new opportunities for the Australian economy, but it also presents some challenges, as explained in chapters 2 and 3.

Figure 6

Age of Australian cyber security providers

Percentage of all providers



Only nine per cent of providers have been operating for **more than 20 years**. Of these, only one-fifth, including ContentKeeper and Huntsman Security, focus exclusively on cyber security.

Survey question: When was your organisation established?
Sources: AustCyber's Digital Census 2020, customised data from illion, Crunchbase

[1] Note: Outliers, such as professional services providers, old IT providers, defence related firms and other providers that have been around for more than 30 years were excluded

[2] Dedicated cyber security providers refer to firms where 100 per cent of revenue and employment can be attributed to provision of cyber security products and services

Reflecting its youth, the sector is dominated by SMEs, with over 88 per cent of providers having fewer than 100 employees

Characteristic of its youth, the cyber security sector is dominated by SMEs, which make up around 66 per cent of providers. One-quarter of the businesses in the sector are micro providers (zero to four employees).

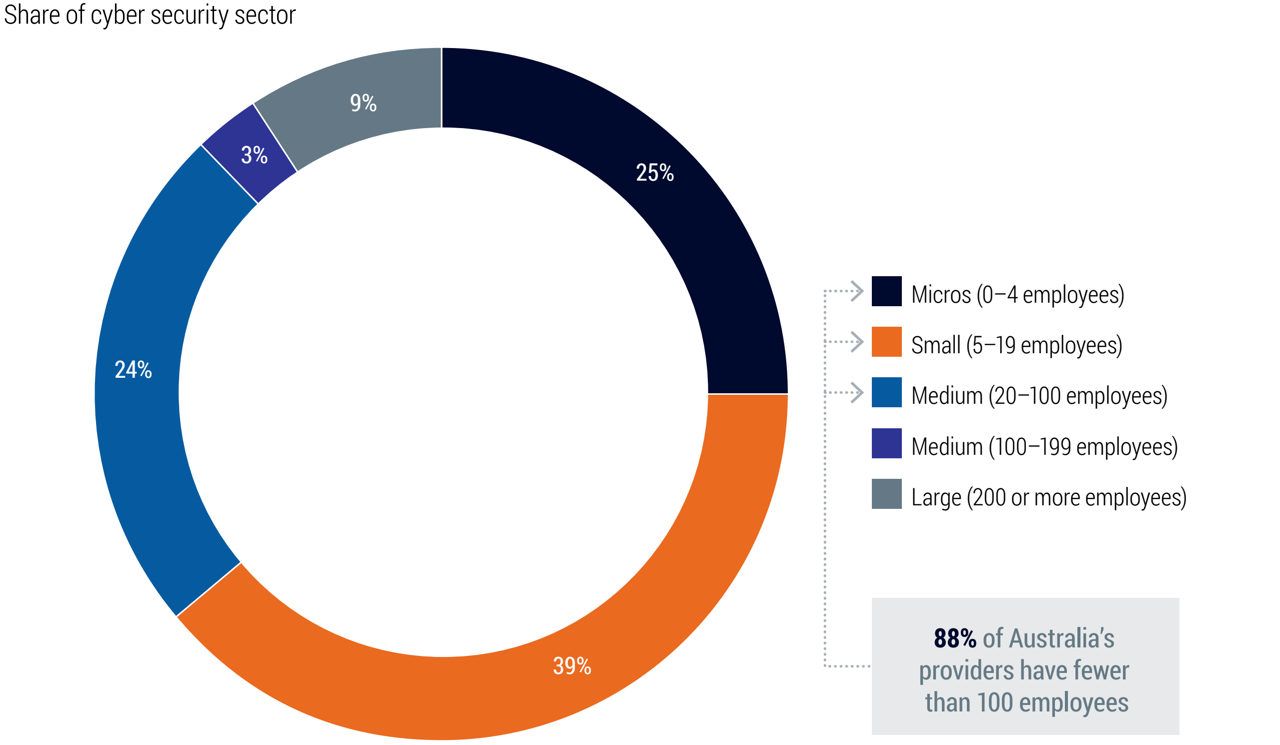
This is expected to change as the sector matures. Of the providers surveyed, 40 per cent report that they plan to expand their workforce over the next 12 months.[1] It is important to remember that this forecast comes at a time of uncertainty due to COVID-19.

Of the providers with 200 or more employees, only 13 per cent identify as dedicated cyber security companies.[2]

The rest of the large cyber security providers are professional services firms such as Deloitte and KPMG; international technology integrators such as Microsoft and IBM; and international defence specialists such as Lockheed Martin and BAE Systems. These larger providers offer cyber security as one part of their overall business, with expert interviews suggesting that cyber contributes five per cent for professional services providers.

Figure 7

Size of Australian cyber security providers



Survey question: What is the current size of your organisation in full time equivalent employees?
Sources: AustCyber's Digital Census 2020, customised data from illion

Australia's cyber security sector includes all cyber security activity that occurs in Australia, where the economic value is added in Australia, including by foreign-owned entities.

[1] AustCyber's Digital Census 2020

[2] AustCyber's Digital Census 2020, expert interviews

Providers specialising in systems security capture the largest portion of Australia's cyber security market

Market spend on cyber security can be broken down by product segment. The largest product segment in Australia's cyber security market is 'Systems security' ($1.5 billion), followed by 'Software and platform security' ($1.3 billion). The 'human, organisational and regulatory' segment has the most providers, with 49 per cent accounting for a key offering. The segment with the fewest providers is 'Infrastructure security', although spending is still $1.1 billion, reflecting how this type of service is geared towards larger cyber providers.

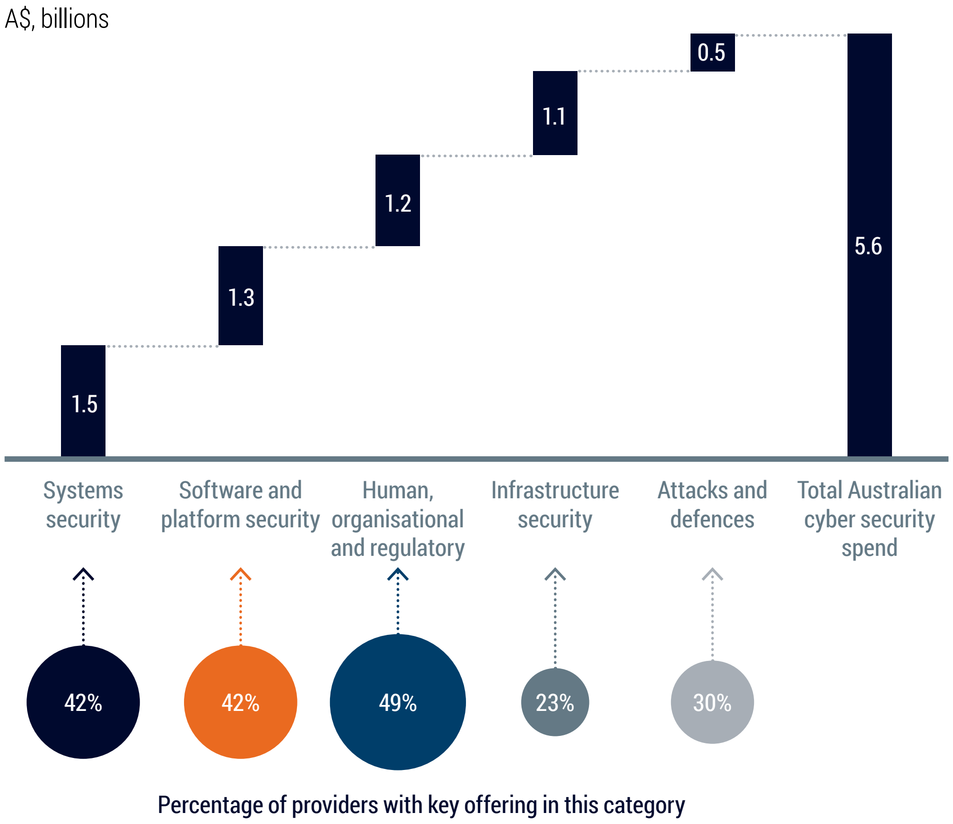
Cyber security, like much digital technology, has traditionally been understood in terms of hardware, software and services. But the diversity and sophistication of modern cyber security means that these categories are no longer appropriate. The Cyber Security Body of Knowledge (CyBOK) is an international collaboration headed by the University of Bristol that structures cyber security according to five main categories:

- **Infrastructure security:** securing computer and digital networks and related physical hardware and systems against intruders.
- **Systems security:** operational, network and systems security that includes the processes and decisions for handling and protecting data assets.
- **Software and platform security:** security that focuses on keeping software and the entire computing platform and devices resilient to cyber threats.
- **Attacks and defences:** a proactive and adversarial approach to protecting against cyber attacks, including performing penetration and vulnerability tests.
- **Human, organisational and regulatory:** tools and services to protect against intentional and unintentional user mistakes, and to ensure cyber governance and compliance.

This new framework provides a more robust foundation for researchers, policymakers and industry to study the sector. See Appendix B for detailed descriptions of each product category.

Figure 8

Australia's cyber security spend by product segment, 2020



Survey questions: What main products and/or services does your organisation offer? Of these, which are your top three products and/or services?
Sources: AustCyber's Digital Census 2020, Gartner, IBISWorld, AlphaBeta analysis

Note: Specialty is defined as the product or service that generates the largest amount of revenue for the business.

The government and defence sectors are the largest customers of cyber providers of all sizes

Analysis of revenue breakdown by industry for both SMEs and larger cyber security providers reveals that although there are minor differences in how revenue is distributed, there are distinct commonalities in how the sector generates its revenue.

For both SMEs and large providers, government (including organisations in healthcare, social care and education) and the defence sector account for approximately 30 per cent of total revenues. 'Government' is the sector's pivotal customer, with nearly 50 per cent of providers surveyed having sold cyber security products or services to the Australian Government over the previous 12 months.[1] This is consistent with the rising cyber threats facing governments such as the growing sophistication of state-sponsored attacks, increasing demand for sovereign cyber capabilities and solutions.

The 'Financial and insurance services' industry is the next major source of revenue, accounting for around 20 per cent for smaller providers and a slightly higher share for larger providers. The financial services sector's appetite for cyber security is driven by the high degree of criminal attention it garners, as well as stringent regulatory and compliance obligations.

It must be noted that this analysis includes only external spending on cyber security. Expert interviews suggest that many of the large providers to the financial services and information and communications technology (ICT) industries are building substantial internal cyber capabilities, as opposed to purchasing external products or services.

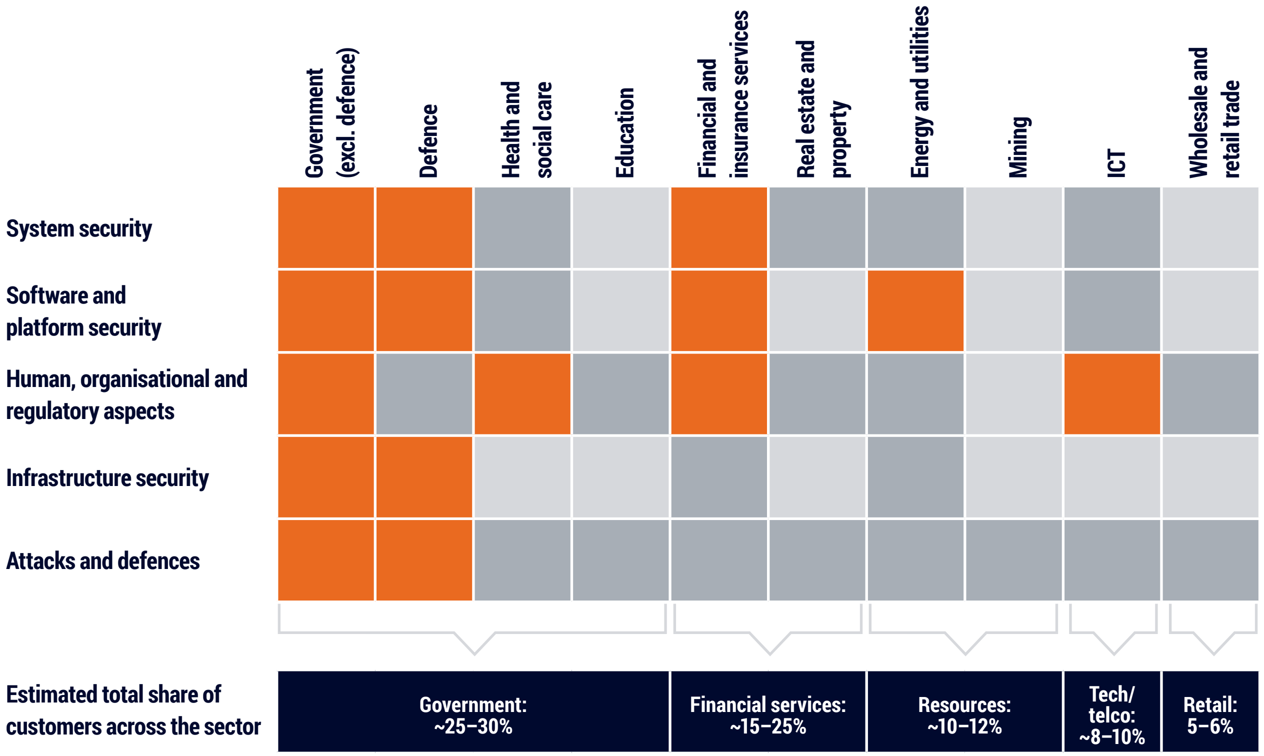
[1] AustCyber's Digital Census 2020

Figure 9

Australian cyber security sector customers by industry

Level of consumption, provider revenue (percentage of total)

Low ░ ▒ 🟧 High



	Government (excl. defence)	Defence	Health and social care	Education	Financial and insurance services	Real estate and property	Energy and utilities	Mining	ICT	Wholesale and retail trade
System security	🟧	🟧	▒	░	🟧	▒	▒	░	▒	░
Software and platform security	🟧	🟧	▒	░	🟧	░	🟧	░	▒	░
Human, organisational and regulatory aspects	🟧	▒	🟧	▒	🟧	▒	▒	░	🟧	▒
Infrastructure security	🟧	🟧	░	░	▒	░	▒	░	░	░
Attacks and defences	🟧	🟧	▒	▒	▒	▒	▒	▒	▒	▒
Estimated total share of customers across the sector	Government: ~25–30%				Financial services: ~15–25%		Resources: ~10–12%		Tech/ telco: ~8–10%	Retail: 5–6%

Note: Data from AustCyber's Digital Census mostly describes SME providers. Data is based on the midpoint of the revenue category survey respondents selected (e.g., estimates $12.5 million revenue if they select $10 million – $15 million). Respondents were asked for the top three products and services they sold and this analysis assumes that revenue out of their top three is split equally across all other products and services they sell. It also assumes that providers' revenue is split equally across the industries they serve. High to low scale is across each product segment only.

Sources: AustCyber's Digital Census 2020, expert interviews

Australia is home to around 350 cyber security providers, with over 80% headquartered in Victoria, New South Wales and the Australian Capital Territory

Figure 10

State-by-state snapshot of cyber security providers

Western Australia's cyber providers are the youngest of all states and territories

Cyber priority areas:

Mining

Oil and gas services

Agritech

Operational Technologies (OT)

Average provider age	7
<5 years	50%
% of providers that export	33%

South Australia has a small number of mature cyber providers with a high export rate

Cyber priority areas:

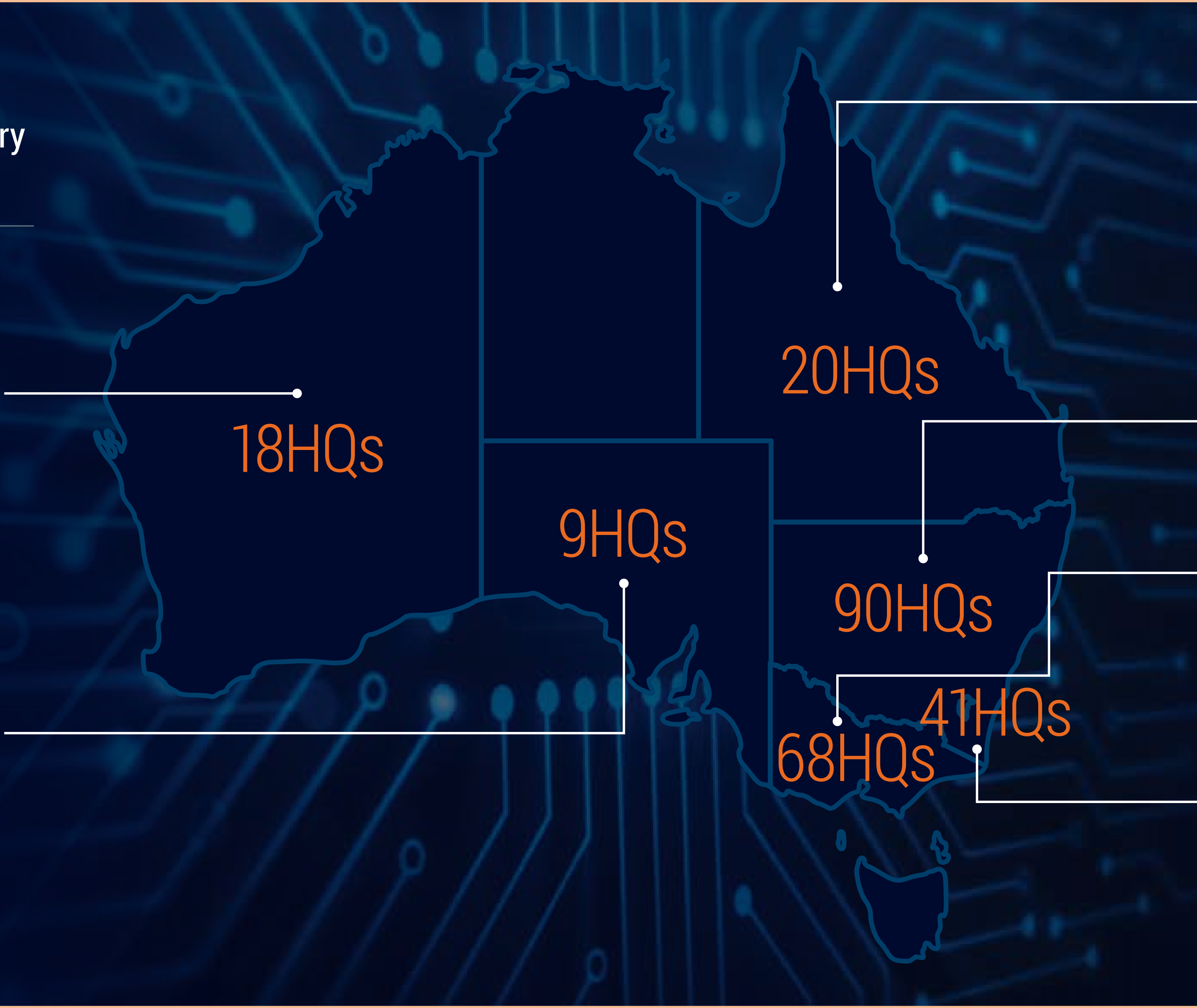
Defence industry and the supply chain

Autonomous systems

Space industry

Digital health

Average provider age	11
<5 years	33%
% of providers that export	67%



Queensland has a small number of mature providers

Cyber priority areas:

- Defence
- Advanced manufacturing
- Health
- Education
- Agritech
- Federal and state government

Average provider age	10
<5 years	32%
% of providers that export	58%

New South Wales is home to the largest and most diverse range of providers

Cyber priority areas:

- Industry 4.0
- Cross sectoral digital transformation
- Cyber workforce development
- Financial services

Average provider age	8.5
<5 years	40%
% of providers that export	38%

Victoria is home to the second-largest number of headquarters for providers

Cyber priority areas:

- Digital health
- Skills and education
- Financial services
- Defence

Average provider age	7.5
<5 years	42%
% of providers that export	46%

Australian Capital Territory providers are focused on servicing the Australian market, with the lowest share of providers exporting

Cyber priority areas:

- Tertiary and research sector
- Defence industry
- Renewable energy
- Federal government

Average provider age	7.5
<5 years	44%
% of providers that export	29%

Note: Cyber security priority areas are the priority capability strengths that have been identified by AustCyber and each state's Cyber Security Innovation Node. Victoria are in the process of establishing a Node, as well as cyber priority areas.

The number of headquarters in each state includes dedicated providers, as well as diversified providers – such as professional services firms, technology companies and defence providers – offering cyber security as part of their business.

The percentage of providers that are exporting and the providers' demographic information is calculated based on where the company is headquartered.

State profiles are based on insights gleaned from AustCyber's Digital Census 2020. No cyber security provider participating in the Census recorded themselves headquartered in Tasmania or the Northern Territory, so these two jurisdictions are not described in this section. As the cyber security sector continues to mature, we expect that Tasmania and the NT will develop their own local hubs.

Sources: AustCyber's 2020 Digital Census, customised data from illion, AlphaBeta analysis

CASE STUDY

Sovereign cyber businesses step up for defence training

Canberra is Australia's defence capital with the largest concentration of defence and national security agencies, assets, organisations, diplomatic networks and industry bodies in Australia. Consequently, opportunity exists for cyber security providers to develop custom solutions to meet defence needs.

In an Australian first, a group of innovative, sovereign cyber companies collaborated to create a successful pilot of a fully online, collective cyber training program for the Australian Defence Force (ADF).

Australian businesses Cydarm Technologies, elttam, FifthDomain, Penten and Retrospect Labs, each with expertise in niche cyber technology, came together to tailor a solution for defence on FifthDomain's cyber training and simulation platform.

The aim of the Accelerated Defence Cyber Training (ADCT) Program echoes the current need for remotely accessible training programs, while also addressing the requirement to rapidly increase cyber skills across defence and industry.

The online training program was conducted from FifthDomain's headquarters in Canberra, and was delivered remotely to Navy, Army and Air Force personnel across the country.

The training was conducted in a highly realistic virtual environment with simulated exercises. Trainees were grouped into virtual teams to remediate vulnerabilities and respond to simulated and real threat actors.

Each cyber business brought their own set of capabilities to create a bespoke solution for the ADF.

Cydarm Technologies deployed their case management platform and dashboard as a command and control system to coordinate team activities and provide oversight for the mentors. Vaughan Shanks, CEO of Cydarm Technologies said, "This enabled trainees in the cyber security operations teams to collaborate on responding to incidents, using playbooks, while the mentors continually assessed their progress."

elttam, an independent security company which specialises in high-quality offensive and defensive security services, played the role of cyber threat actors for the ADF trainees. Matt Jones, Director and Co-founder of elttam said, "We were proud to tailor realistic adversarial scenarios by employing the Tactics Techniques and Procedures (TTPs) found in real world cyber-attacks. The design and execution of each scenario was carefully tailored to give Defence participants the best experience in identifying, learning from, and defending against such cyber threats."

FifthDomain, the project lead and provider of the training and simulation platform, specialises in cyber operations workforce development. Matt Wilcox, CEO of FifthDomain said, "FifthDomain's cyber ranges benefit by being able to integrate niche technologies from our partners to provide Defence the best of breed in Australian cyber innovation. Within the context of COVID-19 limitations, the sovereign, remotely accessible platform enables defence to overcome travel and supply chain challenges to successfully achieve this goal."

elttam CYDARM FIFTHDOMAIN SECURING CYBER SKILLS

penten {retrospect_labs}

Penten enjoyed the challenge of integrating their unique AI generated content and user behaviour on FifthDomain's cyber training platform. Founder and Director of Penten Ben Whitham said, "Although this is only the first step working together, the combined solution of additional realism and automation will enhance the training outcomes, reduce the time taken to create the environments and improve the repeatability."

Retrospect Labs co-designed and facilitated multiple cyber security exercises as part of the ADF's Accelerated Defence Cyber Training course. Jason Pang, CEO of Retrospect Labs said, "We leveraged our unique exercise platform to remotely manage and deliver these exercises to more than 50 ADF trainees dispersed across Australia."

Delivery of this program closely aligned with Australia's Cyber Security Strategy 2020, released in August 2020, which commits A$1.67 billion investment over ten years and outlines a range of initiatives including the growth of the country's cyber skills pipeline as one of its key recommendations.

COVID-19 appears to have hit smaller providers hardest, with medium-sized providers reporting an uptick in demand

The COVID-19 pandemic has driven most economies around the world into recession. The International Monetary Fund expects the global economy to shrink by three per cent this year, while the Australian economy decreased by seven per cent in the second quarter of 2020.

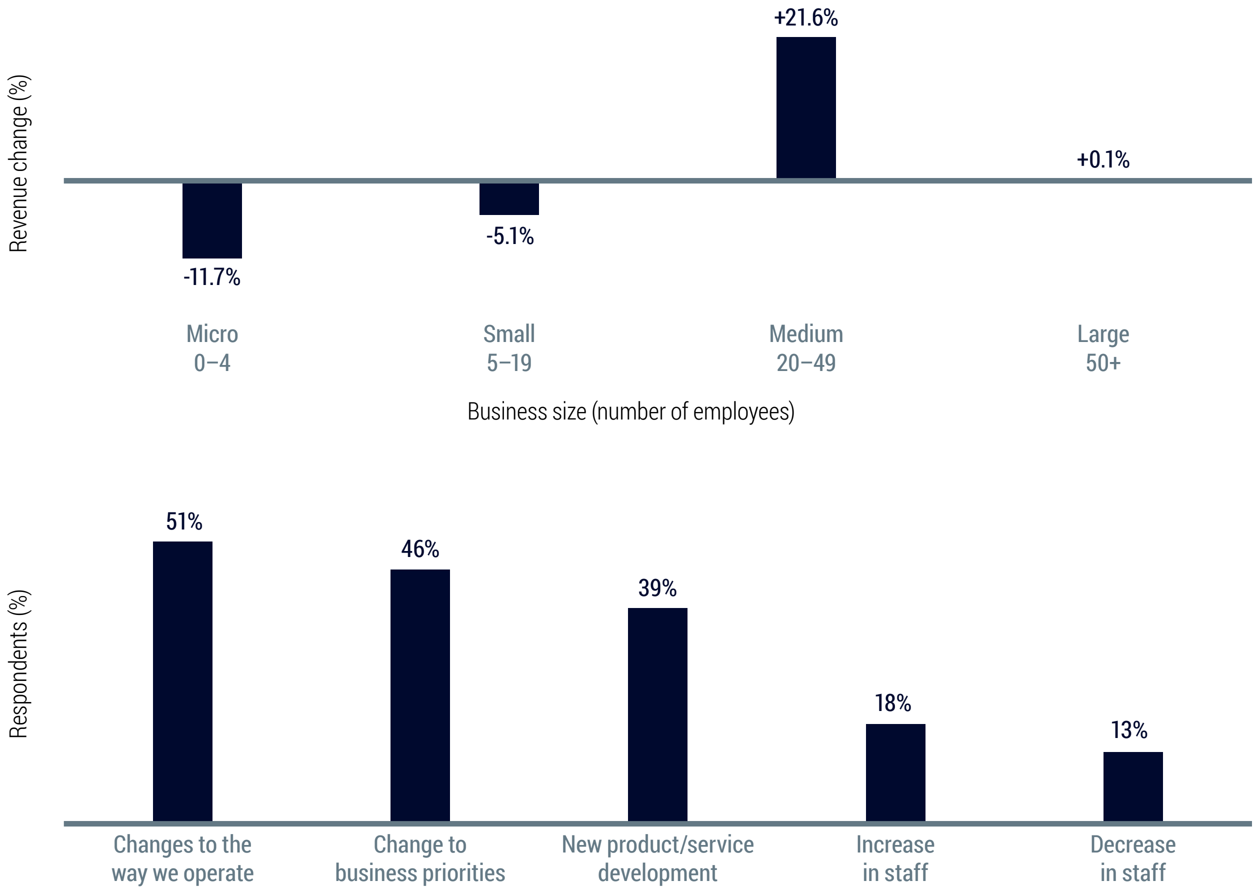
The effects on cyber security are not straightforward. While customers will be restricted in their spending capacity, economies have accelerated their digitisation to cope with social distancing needs. Since social distancing measures came into effect, it is estimated that up to 32 per cent of Australians have been working from home.[1]

Trends such as widespread remote work, e-commerce and the adoption of cloud services are likely to be permanent, which will boost cyber demand in the long-term. Interviews with cyber security providers suggest that while some of their customers are withholding or delaying spending, new customers are seeking to invest in protection as they transition to new digital tools.

Like most businesses, cyber security providers are having to change how they operate – 51 per cent report this as an effect of COVID-19. Encouragingly, providers are also showing strategic flexibility in response to the global pandemic, with 46 per cent of those surveyed reporting a change in business priorities. Furthermore, only 13 per cent reported a decrease in employee numbers as a result of COVID-19, while 18 per cent reported an increase.[2]

Figure 11

Impact of the COVID-19 pandemic on provider revenue, business operations



Survey questions: What is the current size of your organisation in full time equivalent employees? How has COVID-19 impacted your expected business revenue for the 2020–21 financial year? What impact has COVID-19 had on your business?
Source: AustCyber's Digital Census 2020

[1] Roy Morgan Research Centre
[2] AustCyber's Digital Census 2020

"

Trends such as remote work, e-commerce and the adoption of cloud services are likely to be permanent

CASE STUDY

Helping small businesses continue operations

Small businesses face pressure from all directions. With budgets, time and access to expertise constrained, they are constantly on the lookout for technology solutions that can make their lives easier.

Melbourne based company Cynch Security is on a mission to help small business leaders prevent a cyber security incident from becoming one of the worst days of their career.

The team has spent the past nine months helping small businesses across Australia adjust to the changes brought on by the COVID-19 pandemic.

With the shift to working from home for long periods of time, keeping a business secure is a complex undertaking and beyond the reach of those outside the cyber security industry. Attacks continue to evolve and threaten businesses that depend on technology. Advice from experts is often inconsistent and quite generalised, creating confusion and at times, apathy amongst frustrated small businesses.

All of this has resulted in a growing number of businesses concerned about cyber risk, looking for how to best manage it amongst their teams. The responsibility for managing the risk day-to-day often falls to senior leaders with technology operations responsibility. This may be a younger business partner, office manager or the owner themselves if the team is small enough.

Providing micro and small businesses with advice on how to implement risk interventions as businesses transitioned to remote working has been Cynch Security's focus during the pandemic.

"COVID-19 disproportionately affected small businesses, and with increased cyber threats heading their way, we wanted to make sure we did everything in our power to support them when they needed it most," said Co-Founder and CEO Susie Jones.

"We created an entirely new online program for business owners with remote teams to help them manage the new risks they were facing. The program was complemented by a series of blog posts, webinars and supporting resources hosted on our website.

While health risks may have peaked and businesses are now starting to take stock and look towards the future once again, cyber risks remain and continue to evolve. As small businesses navigate these changes, Cynch Security will continue to offer support.

cynch

2 THE NEXT PHASE OF GROWTH

In its next phase of growth, the cyber security sector needs to support rapid digitisation and capture emerging export opportunities

Australia's economy needs to continue to digitise

Driving digitisation in our economy will be critical to improving productivity, living standards and national security in Australia. A maturing integrated digitally connected economy creates greater core interdependencies between technology and sectors. The retail and financial services sectors are well advanced toward digitisation. E-commerce, for example, gives buyers and sellers easier access to multiple platforms, distribution channels, products and services across numerous markets at any one time. New digital technologies such as the IoT, AI and remote operations create new efficiencies and commercial opportunities. Some types of digital technology, such as cloud services and remote working tools, have become critical and indispensable due to the social distancing requirements imposed by the COVID-19 pandemic.

What does the economy need?

The proliferation of digital assets and tools offers new targets for malicious actors looking to harvest data and information for their own interest, putting at risk personal and commercial privacy. A robust and thriving local cyber security sector is therefore essential to support ongoing digitisation in the Australian economy. This is especially important in sectors such as energy, healthcare and research/education, which have been slower to undergo significant digital transformation, but are now under pressure to implement change with increased urgency.

Government has also recognised the need to improve cyber protection, recently flagging the future introduction of baseline levels of cyber resilience across the economy, which will further drive demand for services.[1] While Australian businesses and governments can access some services in the competitive global marketplace, our local cyber security sector plays an essential role. The protection of critical national infrastructure, for example, cannot be sourced exclusively from overseas, due to the national security risks that arise when Australia becomes reliant on foreign providers whose interests may conflict with those of Australia. The concept of sovereign capability does not mean that every component of our cyber protection must be sourced locally, but rather, the local sector has sufficiently sophisticated technical and implementation capabilities to avoid Australian businesses and governments being acutely reliant on foreign providers.

Adapting to secure by design and complex value chains

The traditional concept of cyber security is that – at a broad, conceptual level – its products and services act as a shield that protects digital assets. Other important cyber security offerings, such as risk management and forensics, play their role in mitigating risk, deterring threats and recovering losses when breaches occur. In this way, cyber security is analogous to physical security, where criminals chasing valuable targets are repelled, tracked and investigated. This holds true for much of the digital world and its current suite of cyber-physical systems.

However, a new conceptual approach has emerged for novel technology and systems. Rather than constantly racing to beat cybercriminals before they can exploit security vulnerabilities, digital technology can be built in such a way that it prioritises security and minimises vulnerabilities. This is known as 'secure by design' and reconfigures digital systems so that security is a core criterion that engineers optimise for, rather than being a layer that is added after the fact.

The application of secure by design principles will drive the involvement of cyber security earlier in value chains for many different products and services, and the sector will need to respond to these changes by adopting its services and identifying new customers.

[1] Department of Home Affairs (2020), *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper.* Available at: https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf

A secure by design approach extends beyond individual pieces of digital technology. In the current Australian economy, sectors are increasingly connected – digitally and physically – but with different levels of digitisation and cyber protection. In this new world, it pays to think about security across value chains rather than focusing on the security of individual sectors. The high-profile attacks on Toll Group this year and Maersk in 2018 are early hints at how an attack on one part of a value chain – such as the logistics sector – can impact a host of other sectors across the economy. It is in the rest of the value chain's interest that organisations such as Toll Group and Maersk are secure.

Expanding our export presence

This new concept of cyber security has implications beyond Australia. Understanding how cyber security interacts with other components of the economy is a global issue, especially as so many of Australia's value chains are dependent upon the digital security of other countries.

Increasing Australia's cyber exports to capture a higher share of the US$147 billion global market will be key to the sector's success. Solidifying strong relationships with export markets in the US and UK will draw on our close defence and technology ties. At the same time, expanding into high-potential markets in the Association of Southeast Asian Nations (ASEAN), India and Japan will play into Australia's reputation as a trusted partner and centre of research excellence.

This chapter explores the future of the domestic cyber security sector's growth and its export opportunities.

> "Sectors are increasingly connected – digitally and physically – but with different levels of digitisation and cyber protection

2.1 SUPPORTING OUR DIGITISING ECONOMY

Australia's economy has rapidly digitised over the past decade, unlocking new productivity gains

Digitisation drives productivity gains and business efficiencies much faster than physical industries, unlocking new sources of economic growth for Australia.

The best demonstration of this comes from comparing the performance of digital industries in Australia with physical industries over the past two decades. Productivity growth in digital industries has consistently outpaced that of physical industries, almost doubling total productivity gains over the period. This story is repeated in measure of output and employment growth.

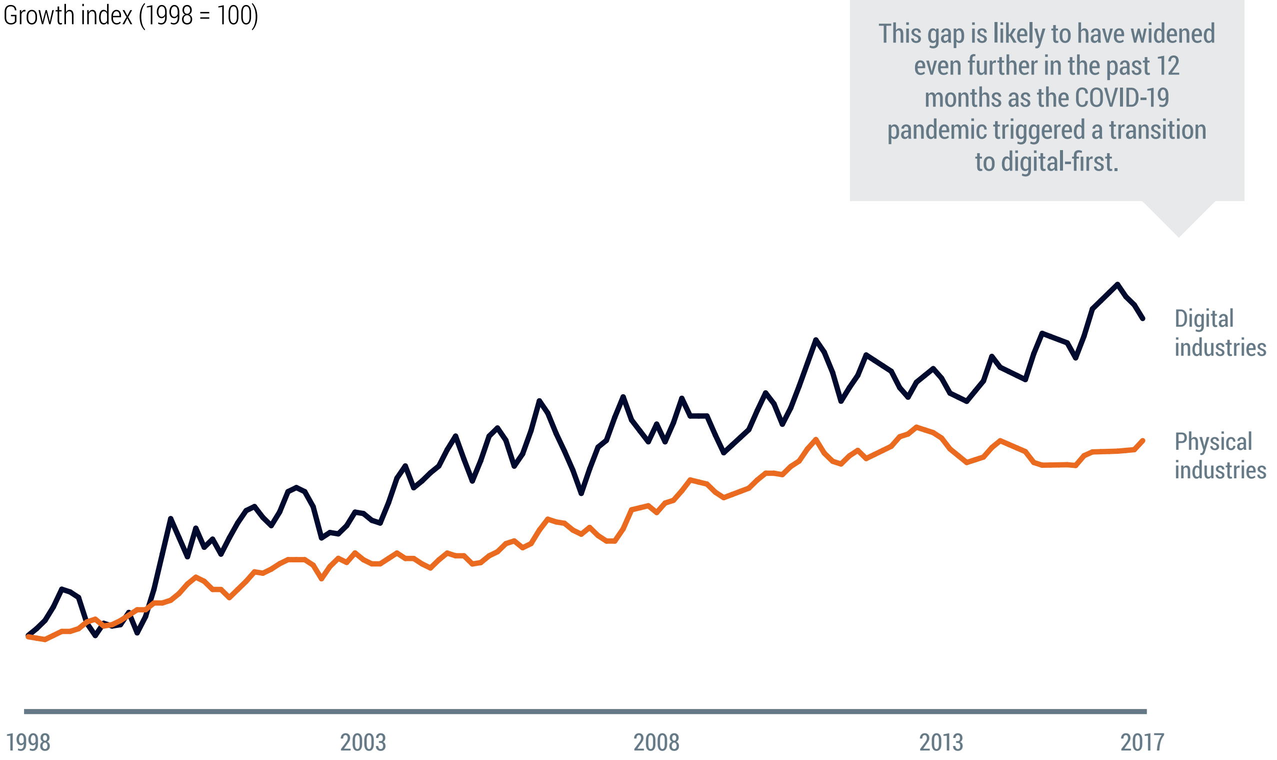
Research also shows the benefits of digitising and automating processes. In Google's 2015 report 'The Automation Advantage', it was estimated that automation could result in $2 trillion in productivity gains for the Australian economy by 2030, leading to millions of safer, more meaningful and more valuable jobs.

The benefits to Australia from its position as a leading digital economy rely on the security, privacy and resilience of its online infrastructure and data. 'Australia's Digital Trust Report 2020' highlighted the critical role digital trust plays in attracting investment and driving jobs growth – adequate cyber security is vital to protecting this trust.

The most rapid digital transformation of the past decade has occurred due to COVID-19, with McKinsey reporting a five-year jump in consumer and business digital adoption within the first eight weeks of the pandemic's worldwide spread.[1]

Figure 12

Productivity in digital and physical industries, 1998–18



This gap is likely to have widened even further in the past 12 months as the COVID-19 pandemic triggered a transition to digital-first.

Note: Methodology is based on Mandel M and Swanson B (2017), *The Productivity Boom*. Productivity is calculated as total output divided by total hours worked. Sources: Australian Bureau of Statistics (2020), *Labour Force Australia*. Available at: https://www.abs.gov.au/statistics/labour/employment-and-unemployment/labour-force-australia/latest-release. Department of Industry, Innovation and Science, Office of the Chief Economist (2018), *Future Productivity March 2018*. Available at: https://publications.industry.gov.au/publications/industryinsightsjune2018/documents/IndustryInsights_3_2018_ONLINE.pdf

[1] McKinsey (2020), *The COVID-19 recovery will be digital: A plan for the first 90 days*. Available at: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-covid-19-recovery-will-be-digital-a-plan-for-the-first-90-days

As the world increasingly digitises, the frequency and severity of cyber attacks has risen

In Australia, the average number of monthly attacks increased by 33 per cent in the first half of 2020. Globally, reports by the FBI and NordVPN cite a 40 per cent increase in daily cyber attacks, compared to pre–COVID-19 levels.[1]

Figure 13 shows the number of cyber security incidents the Australian Cyber Security Centre (ACSC) responded to in 2019–20. This includes malicious emails, compromised systems, data breaches, system shutdowns and malware attacks.

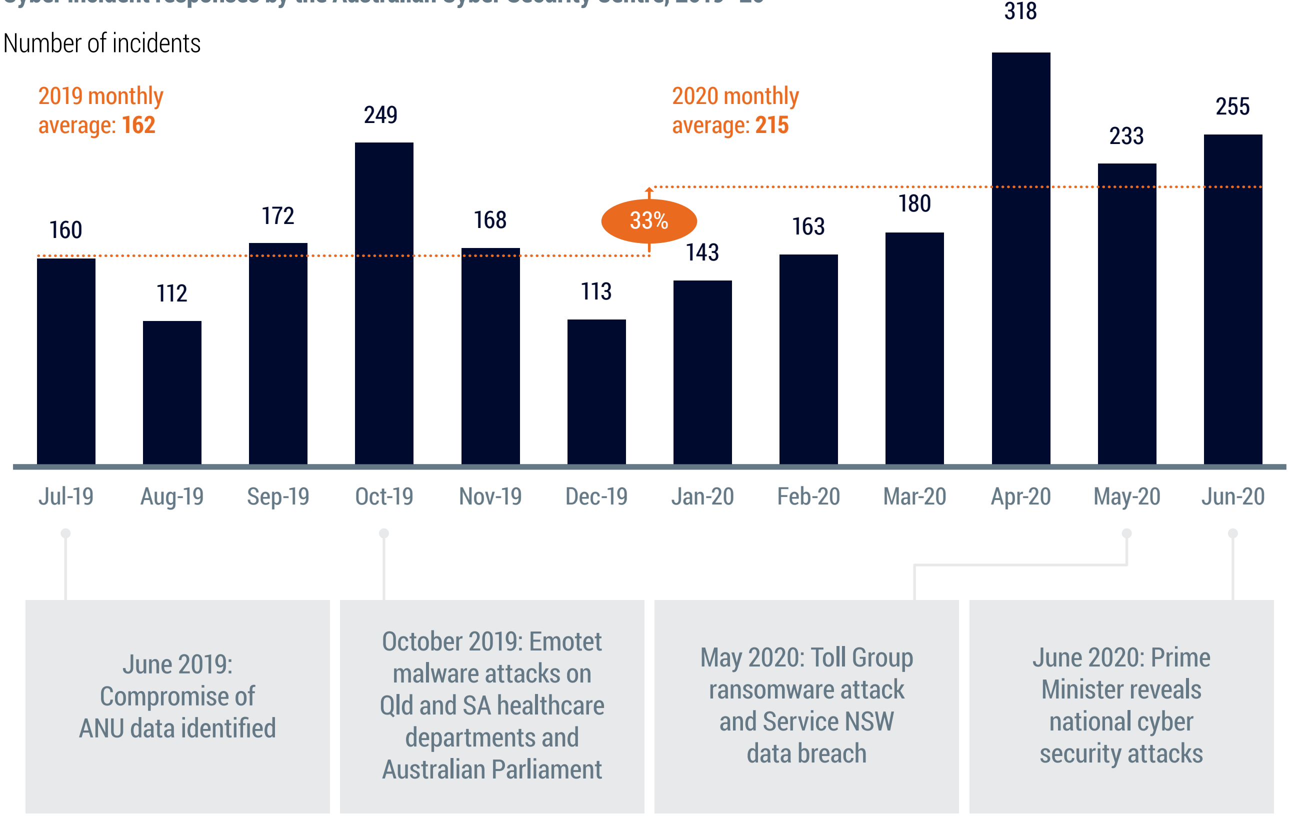
Large businesses reported the most attacks (33 per cent), with SMEs coming in second (32 per cent), followed by the Australian Government and national infrastructure (20 per cent).[2] Significant attacks included:

- compromise of Australian National University (ANU) data in June 2019;
- malware attacks on state government health departments and the Australian Parliament in October 2019;
- a second ransomware attack on Toll Group in May 2020; and
- sophisticated state-sponsored attacks on national institutions, which were revealed by the Prime Minister in 2020.

Awareness of the threats posed by cyber security vulnerabilities increased with the Prime Minister's announcement of state-sponsored attacks, and increased media coverage of cyber security amid COVID-19.

Figure 13

Cyber incident responses by the Australian Cyber Security Centre, 2019–20



Source: Australian Cyber Security Centre (2020), *ACSC Annual Cyber Threat Report: July 2019 to June 2020*. Available at: https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

[1] IT Brief (2020), *Cyberattacks up 400% compared to pre-COVID-19 levels*. Available at: https://itbrief.com.au/story/cyberattacks-up-400-compared-to-pre-covid-19-levels

[2] Australian Cyber Security Centre (2020), *ACSC Annual Cyber Threat Report July 2019 to June 2020*, Figure 2: Cyber security incidents, by categorisation (1 July 2019 to 30 June 2020). Available at: https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

Economy-wide digitisation will generate new threats and demand for cyber security products and services

Figure 14

Five key digital trends ... ... will increase demand for cyber products

New digital technology		Related cyber threats	Systems security	Software and platform security	Human aspects	Infrastructure security	Attacks and defences
Shift to online infrastructure	• Moving services online increases efficiency and productivity, unlocking economic value across sectors	• Moving critical public and private infrastructure online raises vulnerabilities to data theft, service disruption and espionage	▨	🟧	🟧	■	■
Increase in digital payments and fintech	• 61% of Australians make online transactions, increasing the velocity of payments in the economy	• Financial, retail and professional services are heavily targeted by phishing, malware and ransomware	▨	■	■	▨	▨
Proliferation of IoT and smart devices	• IoT allows efficiency gains such as predictive repairing in manufacturing or detecting variations in energy supply on and off-grid	• With 20–30 billion active devices, expanded threat vectors and infiltration risks make IoT devices a target of hackers	▨	■	🟧	■	🟧
Remote access to operations technology (OT)	• Many sectors, such as resources and infrastructure, rely on remote OT. COVID-19 has accelerated trends	• Surges in OT attacks pose risks to intellectual property (IP) and data transitioning between secure and insecure hardware and networks	▨	▨	■	■	▨
Expansion of AI and quantum computing	• AI, automation and other technologies, including blockchain and quantum computing, drive innovation	• Technology innovations raise unknown vulnerabilities to systems, processes, algorithms, data and credibility	▨	■	▨	🟧	■

Sources: Australian Payments Network (2018), *2018 Annual Review*. Available at: https://www.auspaynet.com.au/insights/Annual-Review/2018-Annual-Review. *IBM (2020), IBM X-Force Threat Intelligence Index*. Available at: https://www.ibm.com/security/data-breach/threat-intelligence. *Forbes (2020), 2020 Roundup of Cybersecurity Forecasts and Market Estimates*. Available at: https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/. AlphaBeta analysis

■ Significant increase ▨ Moderate increase 🟧 Limited increase

Industries that are digitising, such as healthcare and manufacturing, need to scale up their digital protections

While demand for cyber security products has been robust and the sector has rapidly evolved, some sectors have seen a mismatch between levels of cyber risk and investment needs and focus by cyber security providers.

Comparing forecast demand and supply helps to identify sectors with a possible shortfall of cyber security products and services, and highlights where the local sector may have to do more to meet the needs of the economy. For example, industries such as government (excluding defence) are likely to have strong future demand met by strong supply, so the incremental cyber security growth requirement is relatively small. Other industries, such as transport and logistics, are forecast to have moderate future demand but low future supply, so the incremental growth requirement for cyber products and services is higher.

Three sectors stand out for very high growth potential:

- Healthcare and social assistance is likely to experience accelerated digitisation due to COVID-19 and increasing attacks on healthcare systems and medical research companies. Protecting patient data and IP will become a higher priority.
- Education is likely to see the integration of online systems and delivery models. Research and student data will become more vulnerable and the moderate planned supply growth by SME cyber security providers may not address the heightened threat level.
- Manufacturing will need substantial new cyber security investment in the wake of Industry 4.0 and transitions to advanced manufacturing methods and technologies, as well as increased threat levels for uptake of IoT. Further demand will come from the Australian Government's Manufacturing Modernisation Strategy and impacts of the pending 'Protecting Critical Infrastructure and Systems of National Significance' legislation.

Note: To estimate potential future cyber security shortfalls, our analysis considered supply and demand. To forecast future demand, three factors were used: digitisation potential, cyber threats and regulated minimum standards. To forecast future supply, historical investment levels and cyber security sector SMEs' growth plans were used.

> "Some sectors have seen a mismatch between levels of cyber risk and focus by providers

Figure 15

Potential cyber security shortfalls by industry

Industry	Possible cyber shortfall	Explanation
Healthcare and social assistance	Very high	Digital health records and telemedecine increasing with growing regulatory obligations; historically, investment is low
Research, education and training	Very high	Digitisation amplified by COVID-19, growing regulatory obligations; historically, investment is low
Manufacturing	Very high	Industry 4.0 will increase exposure to threats, and much digitisation is still to occur in the domestic sector; historically, investment is low
Transport and logistics	High	Moderate digitisation occurring and threats growing (e.g., Toll Group and Maersk); SME providers' growth supply plans are moderately low
Wholesale and retail trade	High	Australian sector will continue to transform through e-commerce and experience increasing threats; limited SME provider plans to grow supply
Energy and utilities	Medium	Slow digitisation and threats, high regulatory obligations; moderately high historical investment and supply growth
Financial and insurance services	Medium	New fintech will increase demand alongside a high threat and regulatory environment; met by existing investment and supply growth
Defence	Medium	Very high threat and regulatory environment; being addressed by strong government investment and supply growth
Professional services and consulting	Medium	Already highly digitised industry with valuable data assets; high historical investment and moderately high planned supply growth
Government (excluding defence)	Low	High threat environment that is digitising rapidly; addressable through continued high investment and SME providers' supply growth plans
Information, media and telecommunications	Low	Medium-high digitisation potential and threats but little regulation; historically, moderately high investment and SME supply growth plans
Mining	Low	High digitisation potential but most needs met internationally; historically, low domestic investment and limited SME supply growth plans

Sources: AustCyber's Digital Census 2020. AlphaBeta analysis. McKinsey Global Institute (2017), *Digital Australia: Seizing opportunities from the Fourth Industrial Revolution'*. Available at: https://www.mckinsey.com/featured-insights/asia-pacific/digital-australia-seizing-opportunity-from-the-fourth-industrial-revolution. ABS (2020), *Australian System of National Accounts*, cat. no. 5204.0, Table 5: Gross Value Added by Industry. Available at: https://www.abs.gov.au/statistics/economy/national-accounts/australian-system-national-accounts/latest-release

As cyber security risks grow, regulation of a broad range of critical infrastructure sectors is tightening

In addition to support for economy-wide digitisation, Australia's cyber security sector must increase the development of specialised sovereign capabilities that protect critical national systems and infrastructure. Addressing these needs requires research, technology development and sovereign hardware manufacturing capabilities, as well as leadership, integration and maintenance.

While some industries have seen strong cyber security investment historically, others – such as those shown on the right – may have relatively less mature cyber security approaches. These newly identified industries – including digital health, food and groceries, transport and 5G – present opportunities for the Australian cyber security sector to grow to supply sovereign defence and protection.

The Australian Government is currently working to implement new regulations to improve the protection of national infrastructure and other critical systems.[1] It is expected that measures will be introduced soon to cover the priority sectors listed in the table and this will drive demand for sector-specific solutions.

Other sectors, such as large Australian technology, mining and retail companies, are also likely to require more of their cyber security goods and services to be supplied locally as supply chains become more localised in the wake of COVID-19. A shift towards secure by design will further contribute to a turn to local, more specialised capabilities.

Figure 16

Protecting Australia's critical infrastructure and tech-adopting sectors

New technologies	Cyber security needs
Telehealth and new digital health systems	• COVID-19 has accelerated digitisation in healthcare, with tele-consults, digital prescriptions and the increasing digitisation of health data and records. This will require accompanying systems security and risk management for patients' private information.
Higher education and research	• Researchers are increasingly working and storing their data in the cloud. This is likely to lead to greater IP and data theft threats and the need for greater protection from malicious actors.
Food and groceries	• Food and grocery supply chains need to be resilient to disruption. As these systems are now highly automated, they can be more vulnerable to cyber security attacks.
Transport and logistics	• Similarly, the transport and logistics sectors need to increase their cyber resilience. High-profile attacks on Toll Group and Maersk illustrate the potentially crippling effect of ransomware and malware.
Telecommunications and 5G	• New telecommunications technology such as 5G presents new cyber security challenges.

Government has identified several industries with nationally critical infrastructure and systems that require proportionate security obligations:

- Banking and finance
- Communications
- Data and the cloud
- Defence
- Education, research and innovation
- Energy
- Food and groceries
- Health
- Space
- Transport
- Water

Source: Department of Home Affairs (2020), *Protecting Critical Infrastructure and Systems of National Significance: Consultation Paper August 2020*. Available at: https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf

[1] Department of Home Affairs (2020), *Protecting Critical Infrastructure and Systems of National Significance*. Available at: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems

Cyber insurance offers businesses a financial mechanism to manage risk, while encouraging investment in cyber security

Insurance has traditionally been a central tool for businesses and individuals to manage risk. However, the digital economy has focused on managing cyber threats primarily using cyber security products and services.

This is changing as insurers are beginning to offer more protections specific to cyber security. Insurance allows the pricing of cyber risks, enabling businesses to compare the costs of cyber products to the cost of breaches and insurance. In this way, businesses can optimise their expenditure across cyber security and insurance.

Insurers are developing a price for cyber risk that allows businesses to transfer their risk. For example, CyberCube in the US prices risk by running specialised analytics on internal and external security data, historical losses and enterprise data. Established cyber insurer Allianz considers potential damages payable due to loss of customer data, the impact of business interruption and loss of reputation when pricing risk.

The two types of cyber insurers that are active in the market are:

a. large international insurers working with cyber risk experts (e.g., Chubb, Axa and Gallagher); and

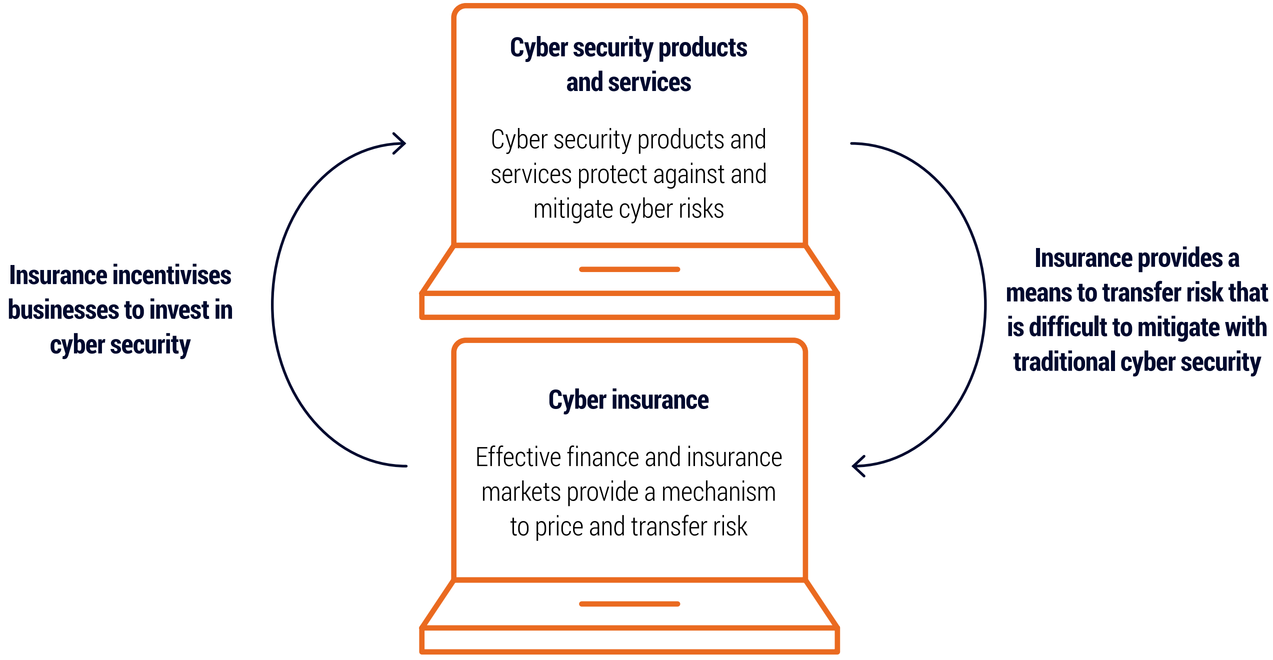
b. specialist cyber insurance providers (e.g., IAG Firemark and Coalition).

Australia's cyber insurance market is only slowly gaining traction: most businesses have not yet recognised the role insurers play in protecting against cyber threats. Developing this market will require lifting awareness of the role of cyber insurance, and may need regulation to stimulate uptake.

Figure 17

Cyber insurance complements security products and services

Risk management combines protection and insurance



Cyber security products and services

Cyber security products and services protect against and mitigate cyber risks

Cyber insurance

Effective finance and insurance markets provide a mechanism to price and transfer risk

Insurance incentivises businesses to invest in cyber security

Insurance provides a means to transfer risk that is difficult to mitigate with traditional cyber security

Examples of cyber insurers

AXA CHUBB Coalition Gallagher iag

2.2 CAPTURING EXPORT OPPORTUNITIES

43 per cent of cyber security companies are already exporting, demonstrating a strong global outlook within the sector

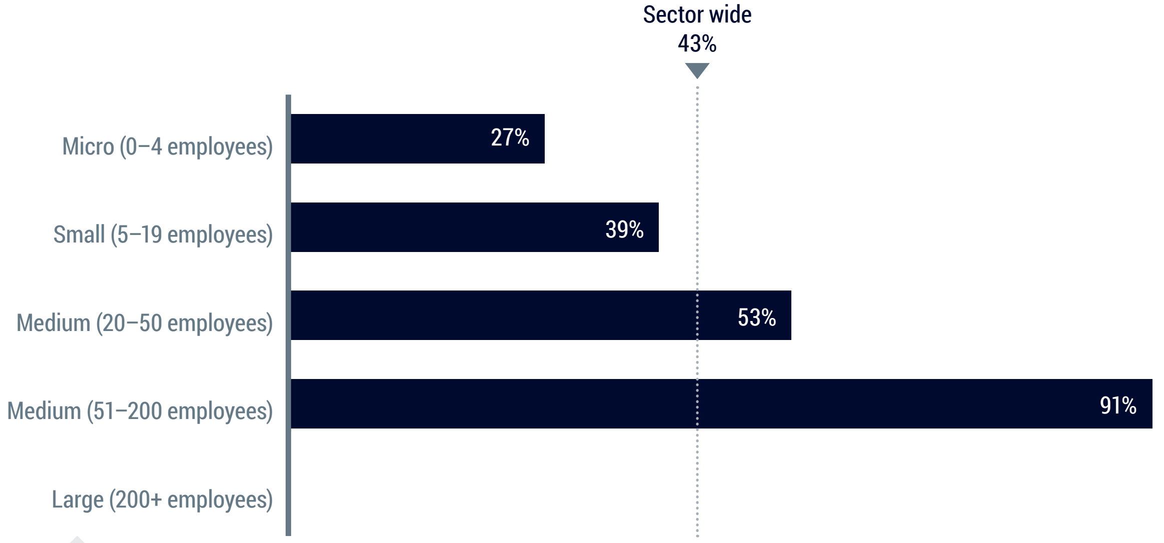
The cross-border nature of cyber security underpins a global market for security solutions. Combined with expansive and complex supply chains, this means that the security problems that companies are solving are global in reach and have the potential to generate attractive revenue.

Crucially, focusing exclusively on local customers is not an effective growth strategy for cyber security companies. While local short-term success and sales are beneficial, it is widely acknowledged that while the scale of Australia's domestic market is sufficient for testing product and service concepts, it is not large enough to sustain companies that can compete with global cyber security providers on an ongoing basis. Startups – especially in software and hardware – must aspire to grow internationally to compete with global providers, even domestically. Cyber security's international environment of threats, providers and intellectual property together drive this requirement.

Around 43 per cent of organisations in the Australian cyber security sector are currently exporting their products and services overseas. This underscores Australia's strong cybertech capability and the ability to connect with global customers. Medium-sized companies with 51–200 employees are most likely to export, but small companies (5–19 employees) are making impressive headway in gaining traction internationally.

Figure 18

Percentage of providers exporting by size



The result for large firms is not conclusive due to a limited sample size; however, large cyber companies may service other markets through local operations or regional bases

Survey question: In the 2019–20 financial year, did you export any products and/or services?
Source: AustCyber's Digital Census 2020

Currently, leading cyber security economies such as Israel and the UK are generating six to 12 times the export revenues of Australia

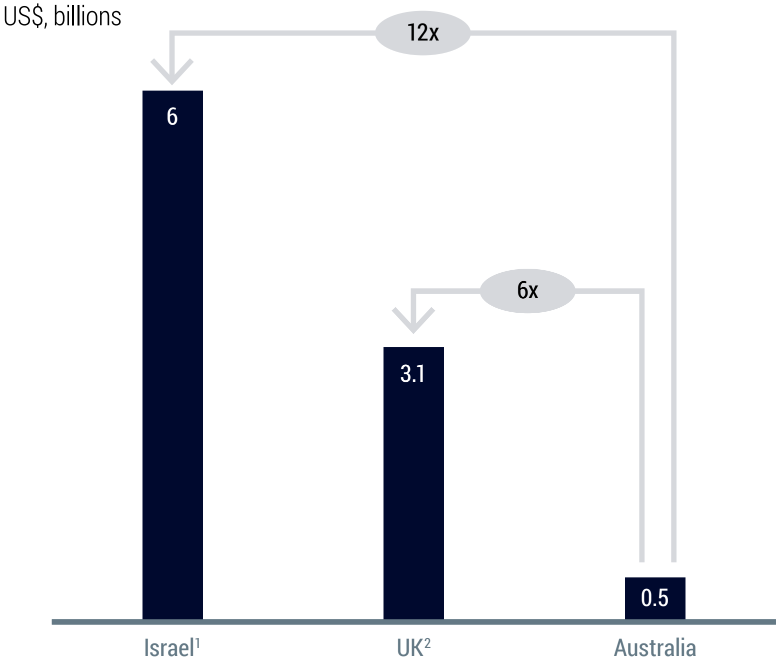
Australian exports now account for 15 per cent of sector revenue, with 43 per cent of providers exporting, indicating that the sector has seen significant growth in exports over recent years. Expanding this export share will help to mature Australia's cyber security sector as revenues increase and companies become established, trusted providers globally.

Marketing Australia's key advantages will be critical to building export revenues. Two of the most marketable advantages include our international reputation for research excellence and our expertise as a trusted defence and security ally through the Five Eyes community. The reputation of Australian businesses as honest and reliable will see them act as trusted providers of products and services internationally.

Due to the global nature of the cyber security opportunity, the sector's ability to capture export opportunities and compete internationally are key to long-term success.

Figure 19

Cyber security export revenue for Israel, UK and Australia



The US, the world's largest cyber security exporter, is home to 24 of the top 25 cyber security companies in 2020.[3]

Compared to Australia's sector, the UK and Israel boast higher export volumes. The UK captures **29 per cent of sector revenue** through exports. Australia can continue to grow exports to compete internationally.[2]

Note: The figure for Israel is based on a 2018 industry report. The figures for Australia and the UK are for 2020.

1. Israel Ministry of Foreign Affairs (2019), *Israeli Cyber Industry Report – Main Findings (2013-2018)*. Available at: https://mfa.gov.il/mfa/innovativeisrael/sciencetech/pages/israeli-cyber-industry-report-main-findings-(2013---2018)-2-september-2019.aspx#:~:text=Capital%20raising%20activity%20in%20the,significantly%20between%202013%20and%202018.&text=Israeli%20activity%20accounted%20for%2018,management%20spending%20(including%20CyberArk)
2. UK Government (2020), *UK Cyber Security Sectoral Analysis 2020*. Available at: https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2020
3. CIO Applications (2020), *Top 25 Cyber Security companies – 2020*. Available at: https://cyber-security.cioapplications.com/vendors/top-25-cyber-security-companies-2018-rid-79.html

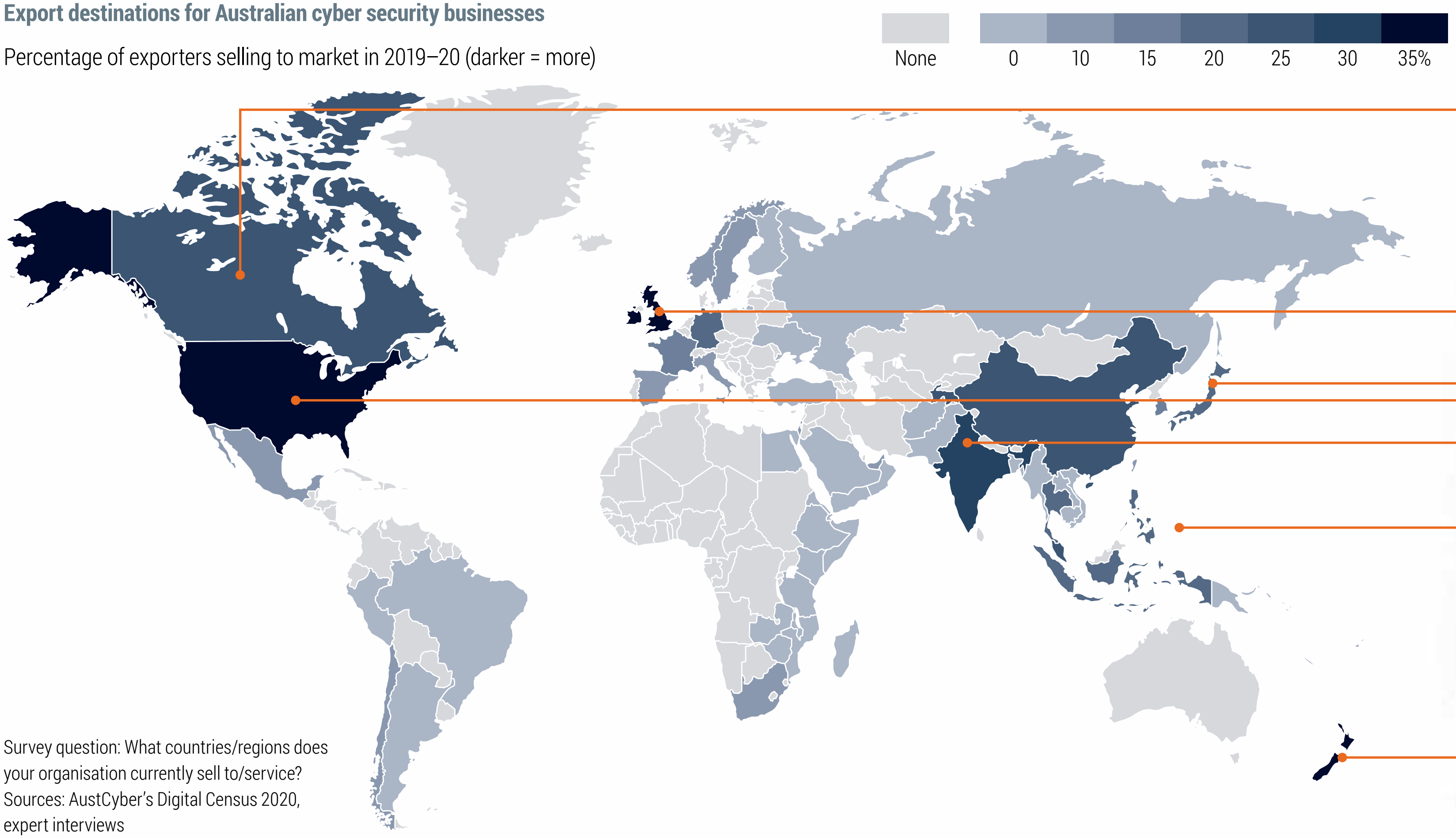
Sources: AustCyber's Digital Census 2020; AlphaBeta analysis

Australia's current largest export markets are the US, UK and Singapore

Figure 20

Export destinations for Australian cyber security businesses

Percentage of exporters selling to market in 2019–20 (darker = more)



Survey question: What countries/regions does your organisation currently sell to/service?
Sources: AustCyber's Digital Census 2020, expert interviews

Canada

- Strong market, but requires development
- Attracts 29 per cent of exporters, seven per cent cited among top three
- Professional and financial services

UK

- Primary market
- **Attracts 43 per cent** of exporters
- Defence and data security

Japan

- High potential
- Attracts 21 per cent of exporters, two per cent cited among top three
- Application and defence security

New Zealand

- Strong market
- Attracts 38 per cent of exporters, 17 per cent cited among top three
- Critical infrastructure, defence and data security

ASEAN

- High potential
- **Singapore attracts 57 per cent of exporters**, but Malaysia, Thailand, Indonesia and the Philippines attracted only 21–29 per cent. Singapore was a top market with 36 per cent, others scored 0–5 per cent
- Broad needs in infrastructure and platform security

India

- High potential
- Attracts exporters, 9.5 per cent cited among top three
- Baseline security needs including infrastructure and systems security

US

- Primary market
- Home to large OT providers
- High access to finance
- **Attracts 64 per cent** of exporters, half cited among top three
- Defence and high-tech; niche solutions

The US and UK should continue to be attractive export markets, with new opportunities in ASEAN, India and Japan

Close alignment between innovation cultures, in addition to clusters of venture capitalists and strong demand markets, have created an established pathway of international expansion to the US and UK for Australian cyber security startups.

Gaining initial success in these key markets can signal the way for broader international expansion, especially into emerging digital giants in Asia. Within these markets, the ASEAN, Japan and India will experience large technological transformation and high growth in demand from digital hungry consumers, and are currently under-serviced by Australian exporters. The recently negotiated Regional Comprehensive Economic Partnership, supporting a significant trading bloc in the Indo-Pacific, will further focus energies in these markets.

However, successfully capturing clients requires businesses to understand the cultural norms of doing business in each country. Partnering with local businesses to navigate the political and cultural landscape is a strong avenue for success. In the Indonesian market for example, almost all new entrants work with Indonesian partners. As such, partnership is a preferred export approach in many markets that have complex political, cultural and business landscapes.

Figure 21

Australia's export opportunities and barriers across target markets

Market		Australia's opportunity	Preferred export approach	Barriers
Five Eyes	1. US	The US is a global cyber innovation and investment leader with high demand for defence and specialised products. Australia's opportunity lies in defence, cyber solutions that address the needs of key industries, and niche solutions that plug gaps not met by major providers.	• Remote • In country to build network	• High setup costs • Lower commercialisation relative to US providers • High regulation
	2. UK	The UK is a mature cyber security market with close cultural alignment to Australia. It has high demand for defence and specialised products, including for financial services and the growing advanced manufacturing sector.	• UK base can service the European Union	• High setup costs • Compliance with data protection laws
Free Trade Agreement	3. ASEAN	Singapore is a global financial centre, home to 4,200 global businesses and the world's second busiest port. It is a target market for high-tech solutions. Vietnam's cyber spend is booming by 16 per cent per year in sectors such as financial services, healthcare, SME and government. It is a target market for baseline security. Indonesia is transitioning to digital in banking, retail, health, infrastructure and public services. It is a target market for baseline and critical security. Philippines has tightened digital information-related legislation, and there is demand from government and privates. Malaysia has strong cyber cooperation with Australia and high demand in finance and telecommunications.	• Remote • Serve from Singapore base • Partner with local counterparts	• Varying regulatory environment • Language and cultural barriers • Inconsistent supporting infrastructure for digitisation
Partner	4. India	India is a fast-growing, global IT hub integrated in global value chains. Service providers have high security needs to meet data protection requirements.	• Partner with local counterparts	• Cultural barriers • Low cyber regulation
	5. Japan	Japan is an established tech giant with growing defence and high-tech industries involving the Internet of Things (IoT), artificial intelligence, blockchain and agri-ICT. It is a target market for high-tech offerings via local partners.	• Partner with local counterparts	• Language and cultural barriers

Note: Specific products and services may require in-country delivery

Sources: Industry and expert interviews, AustCyber (2019), *Cyber Security Opportunities in the ASEAN Region*. Available at: https://www.austcyber.com/resource/cyber-security-opportunities-asean-region. AlphaBeta analysis

> Partnering with local businesses to navigate the political and cultural landscape is a strong avenue for success

Australia's global competitive edge in products and services such as threat intelligence, cloud security and analytics remains under-exploited

The future export potential of Australian cyber products and services can be assessed according to:

- the volume at which they are currently being exported; and
- the opportunities for Australia to develop a global advantage.

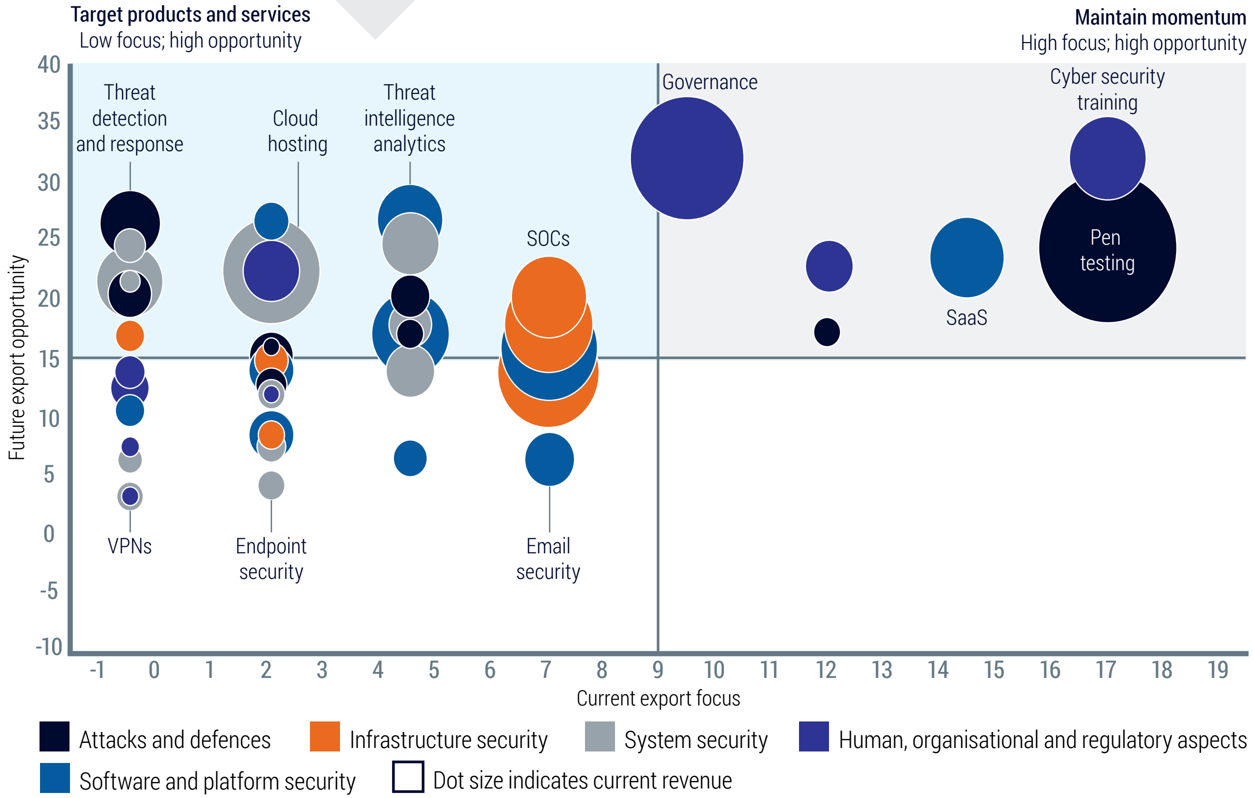
Australia exports a relatively high volume of cyber security training, governance, penetration testing, and security for software as a service. Cyber security providers expect that Australia will continue being globally competitive in these areas. Australia should maintain its momentum and continue to offer high-quality products and services to an increasing number of customers and markets.

Products that are currently rated as being advantageous for Australia, but which we do not yet export on a scale that matches this potential include threat intelligence analytics, threat detection and response, security operations centres, cloud hosting, managed security service providers (MSSPs), cyber readiness assessment and cryptography. These products and services will likely be required by the financial services, mining, advanced manufacturing and healthcare sectors. Increasingly, our export focus towards these high-opportunity products and services presents the ability to match supply to new trends and customers in the future.

Figure 22

Australia's current exports and opportunities to develop a global advantage

Target products include threat detection and response, threat intelligence analytics, cloud hosting, security operations centres, MSSPs, cyber readiness assessment and cryptography.



Survey questions: Thinking about where Australia might focus its energies, in which areas do you think Australia has the most opportunity to become globally competitive? Of the products and/or services that you offer, what were the top three that you exported in FY2019–20?
Source: AustCyber's Digital Census 2020, expert interviews, AlphaBeta analysis

> "Australia exports a high volume of cyber security training, governance, penetration testing, and security for software as a service

CASE STUDY

Australian cyber security innovator Detexian goes global to secure configurations for SaaS applications

Detexian enables small and medium enterprises to manage cyber risks affecting ‘software as a service (SaaS)’ applications such as Office 365, G Suite, Salesforce and Xero.

Founded in 2018, the organisation has established offices in Australia and San Diego, and is exporting to customers in the US, New Zealand, Singapore and Latin America.

Many of Detexian’s customers are small and medium enterprises that provide solutions and services to regulated entities such as large banks, insurance companies and financial services companies. They are heavily reliant on cloud and SaaS technology and handle high volumes of sensitive financial and personal data. Detexian helps these businesses provide proof that security controls are in place at all times to protect their data and gain customer trust.

At the onset, Detexian relied on the word of mouth of their existing customers to win new ones. But the company was quick to leverage the power of digital marketing, social media and strategic alliances to scale its presence internationally.

“Our way to market is quite simple,” said Co-Founder and CEO Tan Huynh. “We have a two-fold strategy to target companies through direct digital marketing and introductions from trusted partners. We’ve also been assisted by AustCyber and The Australian Trade and Investment Commission (Austrade) to connect and meet with potential customers and partners.”

Detexian’s current target export markets are Singapore, New Zealand and the West Coast of the US as there are no issues with timezone coordination, the regulatory environments are mature and business can be conducted 100% online.

In 2020, Detexian has invested significant time and resources studying the Singapore market. “It’s ahead of our home market in terms of infosec regulatory compliance. SMEs constitute almost the entirety of Singapore enterprises, with over 80% having digital transformation strategies in place,” said Mr Huynh. “When we began to target Singapore SMEs through direct digital marketing, we instantly experienced a high degree of interest. Then, through our networks with the help of Austrade, Detexian was introduced to a number of ecosystem partners and potential channels to explore commercial opportunities in Singapore and the wider Southeast Asian region.”

Detexian

The accelerated learnings have helped Detexian refine its business model to further minimise adoption barriers for both SMEs and their trusted partners such as IT consultants and MSPs who can help recommend Detexian solutions to their clients. Detexian is currently in discussions with a number of IT/security consultants and MSPs looking to expand their capabilities.

“In the wider Southeast Asian region, we are entering into strategic alliances with well-known companies with dominating positions in product verticals adjacent to Detexian. These companies are looking to progress in the value chain and jump start their offerings to provide more value-added technologies to their existing clients,” said Mr Huynh.

Australian cyber capability can lead by further integrating secure by design into existing value chains

With the expansion of global value chains and concurrent rise in the costs and severity of cyber attacks, Australia can play a leading role in providing secure by design solutions to domestic and international partners.

The current sales model for cyber security products and services predominantly targets end customers, rather than considering cyber security as a central component in the value creation process.

Integrating secure by design into global digital value chains in sectors such as defence is a proven way for Australian cyber businesses to access international buyers. Expanding global value chains in advanced manufacturing, mining and healthcare are examples of these new avenues for Australian cyber to offer security products and secure by design services in product development and across logistics, operations, marketing and service.

In the future, especially as more companies and industries adopt a secure by design approach to their own digital products and services, there will be opportunities for cyber providers to partner with companies across industries to help them develop products and services that are secure by design, rather than selling cyber security products and services directly to the company and their customers separately.

With new technologies, platforms, products and systems constantly in development, building expertise in secure by design principles will help position Australian cyber to lead into the future, both in global value chains where Australia is a key player and in industries where Australia has a strategic competitive advantage.

Figure 23

Protecting new digital value chains through secure by design

Case studies of global value chains, using example partner countries

Secure by design can be implemented across the value chain

Global value chain examples	Inbound logistics	Operations	Outbound logistics	Marketing and sales	Service
Advanced manufacturing	Supplier compliance in importing inputs from China and Malaysia	Manufacturing products via secure systems in Australia	Distributing products safely to Singapore, maintaining customer and internet protocol integrity	Managing sales from secure sales centres in the Philippines	Providing secure remote servicing opportunities from India
Mining equipment, technology and services (METS)	Original equipment manufacturer (OEM) compliance in importing electrical machinery from Japan	Remote operation of driverless vehicles in the Pilbara from Perth, Western Australia	Exporting to ASEAN, New Zealand and Papua New Guinea (PNG) with secure logistics via trains and ports	Online contract management and sales management largely automated	Secure online contract and buyer management services provided via Australia
Medical	Patient product customisation request transferred securely	Customised medical product manufactured in Australia	Contractors complying with security requirements distribute product back to hospital or general practitioner	Marketing of customised solutions driven from ASEAN	Guarantees and warranties administered by outsourced partner in the Philippines

Sources: Porter's Value Chain model, expert interviews, AlphaBeta analysis

Significant new technologies are being developed and tested in Australia, opening the door for cyber providers to create new security solutions

Groundbreaking new technologies – often described as 'deep tech' due to their reliance on major advancements across multiple fields – create new value chains that require secure by design security approaches.

Australia is involved in developing and testing new deep technologies, including drone delivery, smart remote monitoring, satellite tracking, quantum encryption and autonomous mining. Innovative companies including Wing, Flirtey, Taggle, Rio Tinto and Fortescue Metals Group (FMG) are pioneering world-first tests of new technology, bringing improvements to business and government, as well as increasing consumer satisfaction.

However, each of these new technologies poses new security risks and potential vulnerabilities, requiring close assessment and the involvement of cyber security professionals to ensure products are secure by design. Guaranteeing the security of these new technologies will be critical to their uptake and expansion.

Australian cyber security companies can move ahead of the rest of the world by working with innovators to ensure the security of novel technologies is built in from the beginning. Deep technologies and the ecosystems that support and secure them are critical to the future competitiveness and growth of the Australian economy and our national identity as a key global innovation player.

Figure 24

Protecting new digital value chains through secure by design

New technologies being developed in Australia

Technology and developer	Example	Security needs	Peer countries involved in development
• **Drone delivery** (such as Wing and Flirtey)	• Small automated drones can deliver food, other groceries and pharmaceuticals to underserved areas. For example, Wing is trialling delivery in suburban Canberra.	• End points (drones) • Network and signal security • E-payments • Customer data protection	• Finland • United States
• **Remote sensor monitoring** (such as Taggle)	• Automatic meter reading and IoT sensor technologies can manage water, waste and other resources. For example, Taggle's smart water networks in local council areas in Queensland and NSW.	• End points (IoT) • Analytics software • Data storage	• Japan • United States • France
• **Autonomous mining** (such as Rio Tinto, BHP and FMG)	• Autonomous mining vehicles remove driver error and improve safety by increasing the automation of trucks, drills and trains.	• Remote operating systems • Network and signal security	• United States

Sources: Cicada Innovations, Wing Aviation, Taggle.com.au, AlphaBeta analysis

3

ACCELERATING AND SUSTAINING GROWTH

The cyber security sector has grown quickly, but must confront important challenges relating to innovation, customers and skills

The sector is well positioned to sustain its growth

The remarkable progress the sector has made reflects the importance of cyber security to the modern digital economy. Spending on cyber security has grown by nine per cent each year for the past four years, and in the three years between 2017 and 2020, the cyber security workforce added approximately 4,000 workers (for a total of 26,500 workers).

The demand drivers that have fuelled sector growth – a dangerous threat landscape, digitisation and regulatory demands from government – have been intensified by the effects of the COVID-19 pandemic.

The Australian economy will require sophisticated cyber protection to protect its assets. Risks to the operation of critical national infrastructure – such as power stations, healthcare systems and logistics networks – will grow as digital infrastructure continues to roll out. As online transactions and communications become more common, improper protection could erode digital trust.

Australian cyber security providers need to continue being globally competitive. A high-performing sector prevents Australians becoming overly reliant on foreign providers and enables the nation to capture valuable export opportunities. It also equips Australia with a competitive edge over peer nations in a capability that is critical for a modern digital economy.

As the sector seeks accelerated growth, it needs to overcome familiar challenges.

A survey of cyber providers revealed the following constraints:

- **Knowledge infrastructure:** cyber providers are disconnected from an ecosystem of cyber-orientated professionals in finance, services, policy and education, which hinders innovation in the sector.
- **Market maturity and access:** under-protected businesses and conservative procurement processes that favour established multinationals mean that many local providers struggle to gain traction in their own home market.
- **Investment:** insufficient investor activity means that many providers are reliant on organic growth and do not have the fuel they need to expand their operations ambitiously.
- **Skills:** the sector may struggle to maintain a sustainable, high-quality pipeline of skills which match employer needs.

To ensure these challenges are met, industry, policymakers, investors and educators must continue their proactive efforts to:

- **nurture the innovation environment** by continuing to fund research, in turn helping to mature knowledge infrastructure and expand the investment pipeline for Australian entrepreneurs;
- **help providers and customers connect**, by supporting new providers, scaling existing Australian providers, strengthening the sector's export-oriented outlook and supporting regulations that ensure the digital economy is cyber secure; and
- **sustain skills systems** by continuing to build on the training packages and initiatives that have already been rolled out successfully.

The sector cites demand maturity, a lack of investment and limited access to skills as some of its top challenges

While Australia's cyber security sector is establishing itself quickly, it faces several challenges typical of a young, growing industry that has established a foothold but is looking to scale.

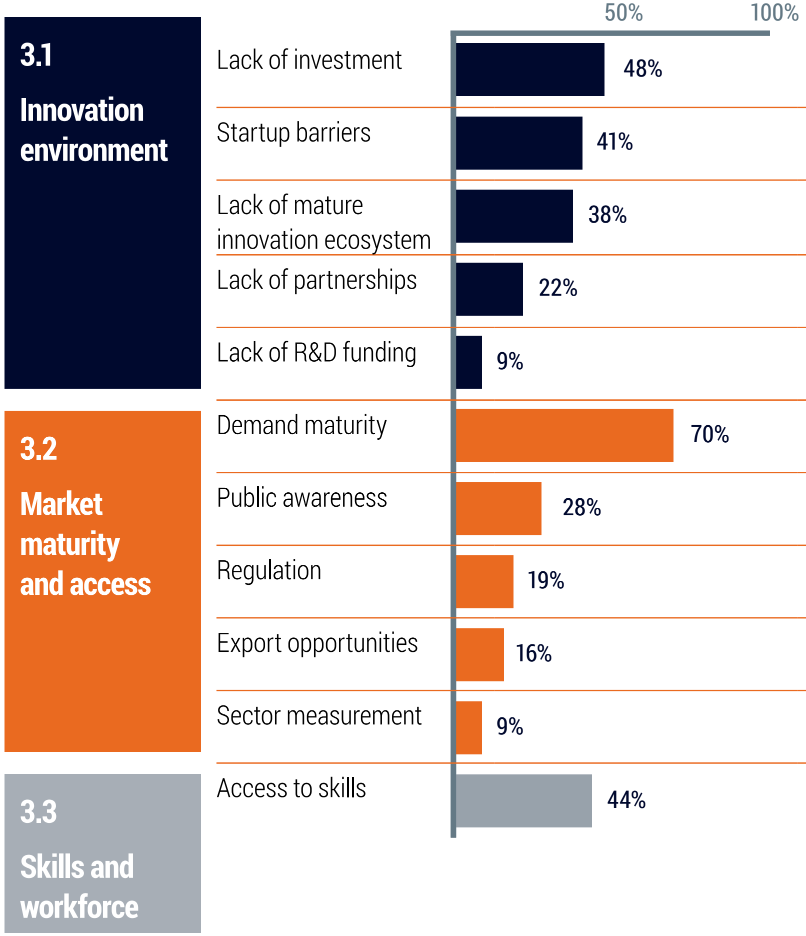
The challenges the sector faces relate to three broad themes:

1. Innovation environment: the ability for organisations with problems to meet people with ideas and develop solutions.
2. Market maturity and access: the quantity and quality of cyber security products and services demanded in the market, and how well local cyber providers can take advantage of that demand.
3. Skills and workforce: cyber security businesses' ability to access the skills they need to innovate and grow.

These challenges have evolved over time and demonstrate the increasing maturity of the sector. In the past, issues such as limited access to cyber skills and lack of R&D funding have been more significant concerns. However, as the industry begins to make progress against these continuing challenges, cyber businesses are also facing new challenges such as the maturity of the businesses they sell to and the amount of early-stage funding available to them.

Figure 25

Top three challenges cited by Australian cyber security providers



3.1 Innovation environment	Lack of investment	48%	Startups report difficulty accessing capital – particularly early-stage and seed funding
	Startup barriers	41%	Startups struggle to access supportive services (e.g. legal, tax), customers and a network of support
	Lack of mature innovation ecosystem	38%	Entrepreneurs can't easily connect to investors, staff and partners due to lack of startup culture
	Lack of partnerships	22%	Lack of partnerships an issue for about a fifth of providers
	Lack of R&D funding	9%	R&D support and incentives still an issue for some providers
3.2 Market maturity and access	Demand maturity	70%	Buyers not 'understanding' what they need is the biggest challenge
	Public awareness	28%	Lack of public awareness is somewhat of a barrier, but is improving
	Regulation	19%	Regulation supporting demand was more typically cited as an enabler
	Export opportunities	16%	Export opportunities are a challenge for about a sixth of providers
	Sector measurement	9%	Sector measurement was not highlighted as major problem by most providers
3.3 Skills and workforce	Access to skills	44%	Limited access to specific types of skills was highlighted as moderate barrier

Survey question: In your opinion, what are the key challenges facing the cyber security industry?
Source: AustCyber's Digital Census 2020

Although cyber security companies face common challenges in demand and investment, those growing fastest are focused on talent and collaboration

Dividing revenues by the age of the provider made it possible to separate responses from the fastest growing companies and those growing more slowly, painting a clearer picture of performance drivers in the sector.

The key growth enablers that fast-growing companies prioritise are gaining highly skilled talent dedicated to growing the company's capability, and harnessing collaborations and partnerships to drive growth. The major concerns shared by these companies include access to skilled talent and maturity of demand.

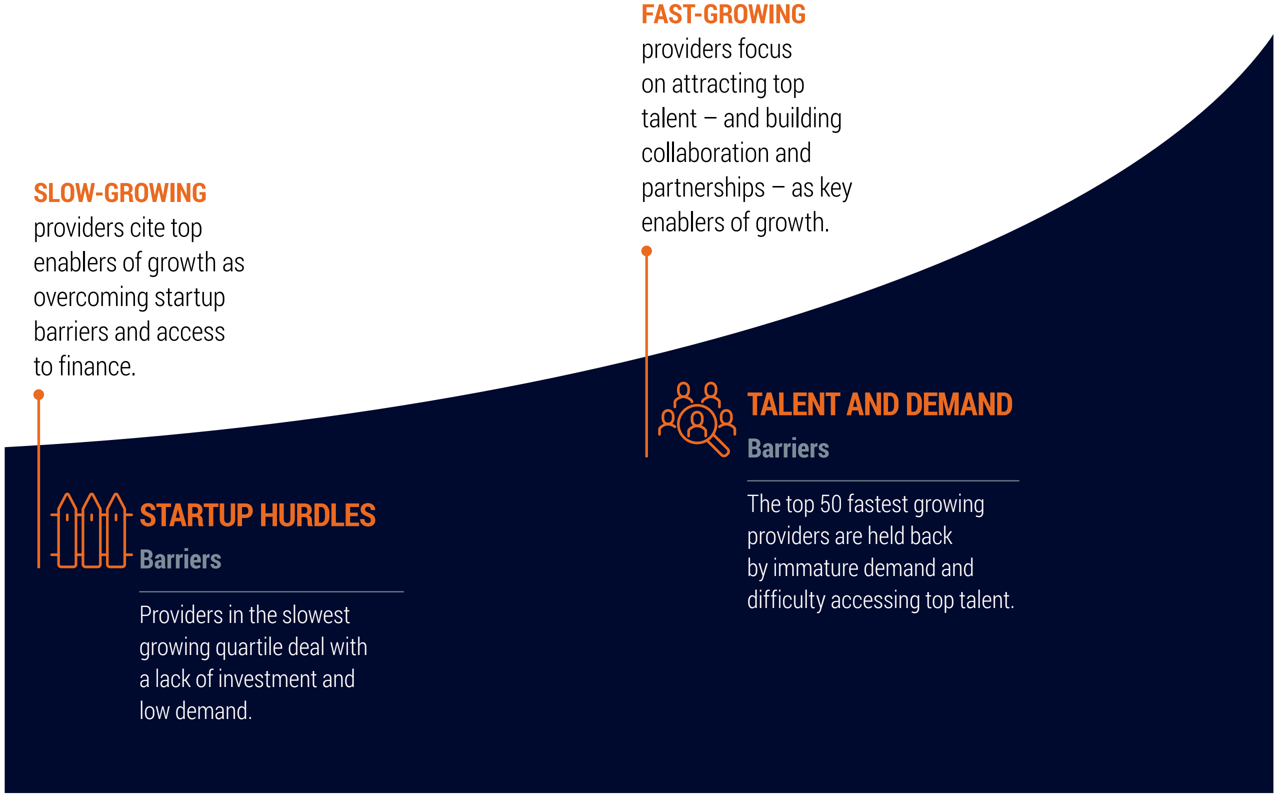
The slowest growing companies are preoccupied with startup barriers and access to finance. These barriers hold them back from taking up export opportunities and zeroing in on talent acquisition.

Overall, the fastest growing companies found it easier than the slowest growing companies to attract talent, engage in R&D, receive market support, gain access to export markets and secure finance. The largest difference in ease was in accessing export markets, suggesting that being able to take up international export opportunities is a key driver of growth.

Figure 26

Barriers and enablers cited by slowest and fastest growing companies

Top barriers and enablers



FAST-GROWING providers focus on attracting top talent – and building collaboration and partnerships – as key enablers of growth.

SLOW-GROWING providers cite top enablers of growth as overcoming startup barriers and access to finance.

TALENT AND DEMAND
Barriers

The top 50 fastest growing providers are held back by immature demand and difficulty accessing top talent.

STARTUP HURDLES
Barriers

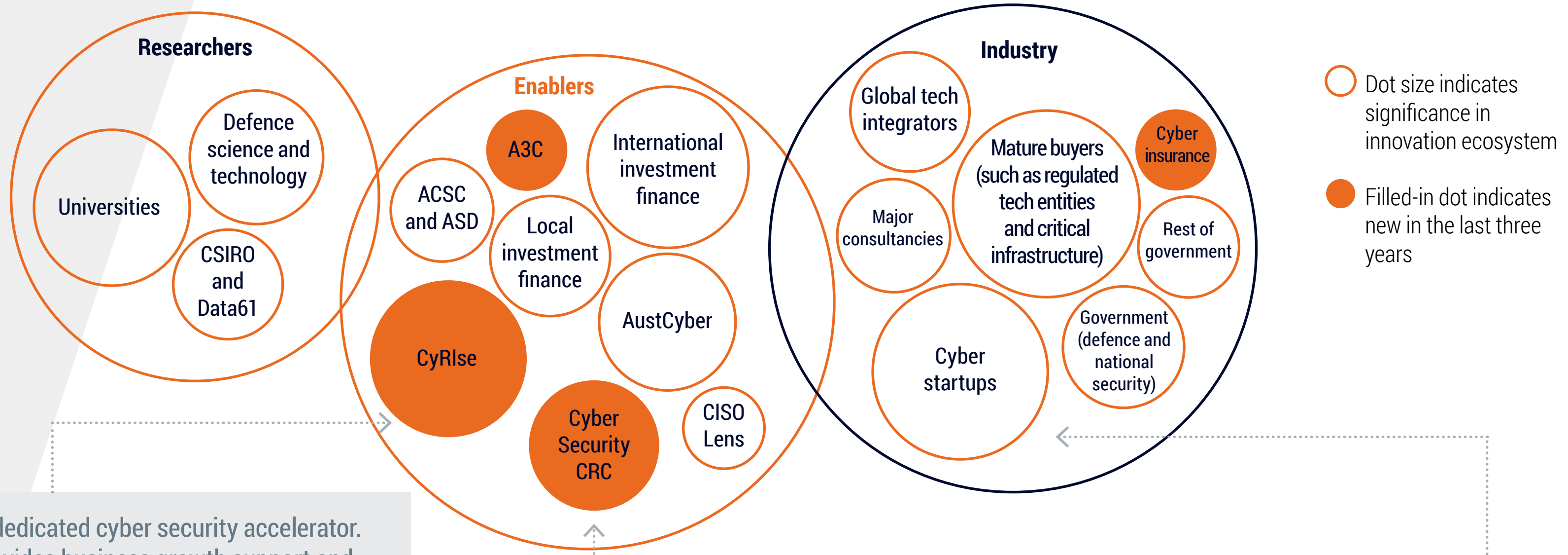
Providers in the slowest growing quartile deal with a lack of investment and low demand.

Survey questions: In your opinion, what are the key challenges facing the cyber security industry? What are the most important enablers of growth for your business?
Source: AustCyber's Digital Census 2020, AlphaBeta analysis

3.1 INNOVATION ENVIRONMENT

As the cyber innovation ecosystem has matured over the past three years, CyRise, the Cyber Security Cooperative Research Centre (CRC) and cyber insurance market innovations have been important additions

Figure 27


Researchers
Universities
Defence science and technology
CSIRO and Data61
Enablers
A3C
ACSC and ASD
International investment finance
Local investment finance
AustCyber
CyRIse
Cyber Security CRC
CISO Lens
Industry
Global tech integrators
Mature buyers (such as regulated tech entities and critical infrastructure)
Cyber insurance
Major consultancies
Rest of government
Government (defence and national security)
Cyber startups
○ Dot size indicates significance in innovation ecosystem
● Filled-in dot indicates new in the last three years

- CyRise is Australia's only dedicated cyber security accelerator. Established in 2018, it provides business growth support and pre-seed funding for up to two cohorts annually.
- The Australian Cyber Collaboration Centre (A3C) was established in 2020 by the South Australian government as a way for industry to better engage with cyber security's application to business strategy and process.

- The Cyber Security CRC facilitates research project collaborations between industry, researchers and government.
- It was established in 2018 with $50 million of Australian Government funding over seven years, and co-funds research projects with industry. It also sponsors research students.

39 per cent of Australian cyber security startups collaborate on R&D.

Note: This diagram is non-exhaustive and indicative only. For example, some industry players are collaborating directly with researchers, so comparing dot size, investment or funding across the sub-sectors does not necessarily indicate the importance of each element.

Sources: Industry and expert interviews; AlphaBeta analysis

Cyber security research funding is growing in Australia, but must continue deepening to support sector innovation and growth

Between 2018 and 2020, cyber security research attracted approximately $64 million of federal government funding. This represents substantial growth from previous levels. During this time, the Australian Research Council (ARC) allocated more than three times the amount of funding compared to the previous three-year period.

For the first time, this level of funding is now on par with comparable economies such as Singapore and Canada, which allocated $61 million and $48 million respectively, also between 2018 and 2020.

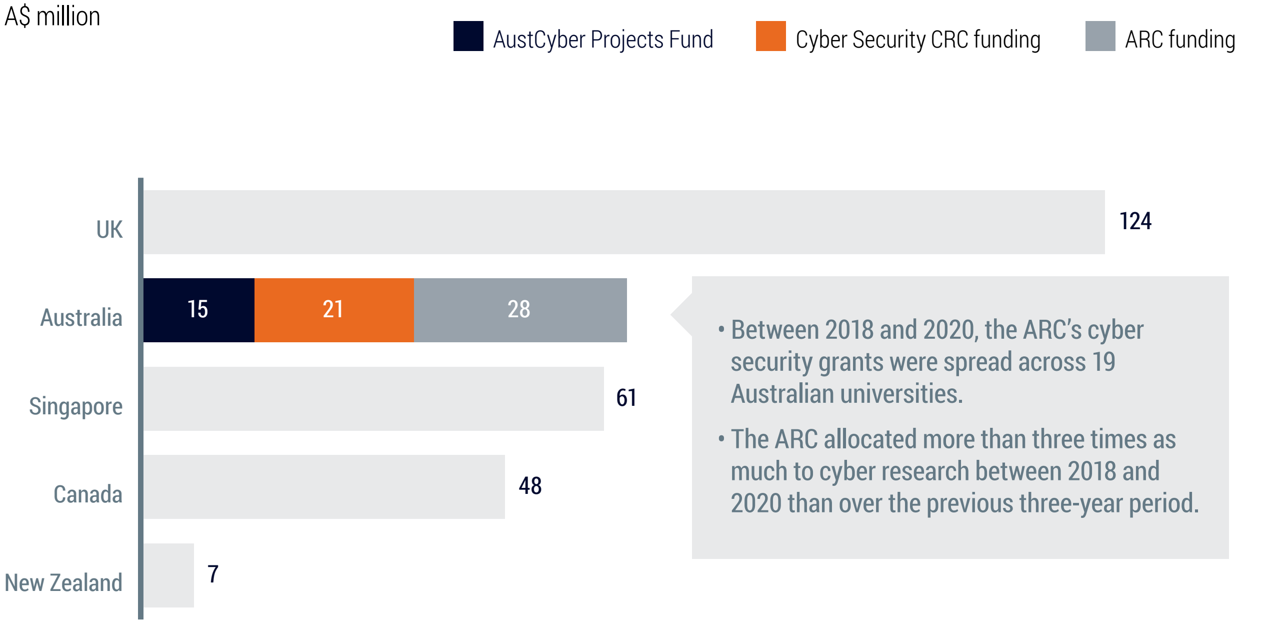
An integral part of the recent growth in Australian cyber security research funding has been the establishment of the Cyber Security CRC. The Cyber Security CRC is the sector's central research organisation, and has a long-term focus on important issues such as critical infrastructure security and cyber security as a service. The CRC has more than 20 partners from industry, government and research, including six leading Australian universities, all of which are required to contribute funding.

Importantly, the Cyber Security CRC has improved the level of collaboration between universities and industry, with expert interviews suggesting that collaborative research approaches are becoming more prominent.

Australia must continue to develop its ecosystem of researchers and, as illustrated by the success of the Cyber Security CRC model, collaboration between academia and industry is key. Furthermore, the broader research sector should be alive to the ever-evolving scope and scale of cyber security discourse and address pressing matters in a timely manner for the benefit of the broader community. The UK, for example, hosts 19 Academic Centres of Excellence in Cyber Security Research and four government-supported cyber research institutes.[1]

Figure 28

Government funding directed to cyber security research between 2018 and 2020



- Between 2018 and 2020, the ARC's cyber security grants were spread across 19 Australian universities.
- The ARC allocated more than three times as much to cyber research between 2018 and 2020 than over the previous three-year period.

Note: Funding includes money allocated to universities or other research institutions. ARC figures include both Discovery and Linkage projects. CRC figures are based on $50 million of government funding over the seven years to 2025. Individual funding from the Cyber Security CRC's members is not included as this is not classified as government funding.

Sources: Australian Research Council, Cyber Security CRC, AlphaBeta analysis

[1] University of Bristol (2020), *The Future of the UK's Cyber Security Research Position in the World.* Available at: https://www.imperial.ac.uk/news/202413/the-future-uks-cyber-security-research/

Increasing numbers of cyber security companies are being established in Australia

Australia's cyber security sector is young, but growing quickly. The growth in number of companies is consistently higher than growth in the wider economy, as well as in comparative sectors such as the information, media and telecommunications (IMT) sector.

Between 2012 and 2019, the number of companies in the cyber sector grew by an average of 21 per cent each year, compared to just two per cent and one per cent each year for the IMT sector and the whole economy, respectively. 53 per cent of Australia's cyber companies were established in 2015 or later.

The growth rate in the cyber industry has also been more resilient to falls in overall activity. For instance, in 2013 when the wider economy experienced a decline across companies overall, the number of cyber companies continued to grow strongly, albeit at a lower level (see Figure 29).

The cyber security sector's company number growth rate is also more volatile than the wider economy's growth rate. This is characteristic of less-mature sectors that are still finding a dynamically efficient competitive equilibrium.

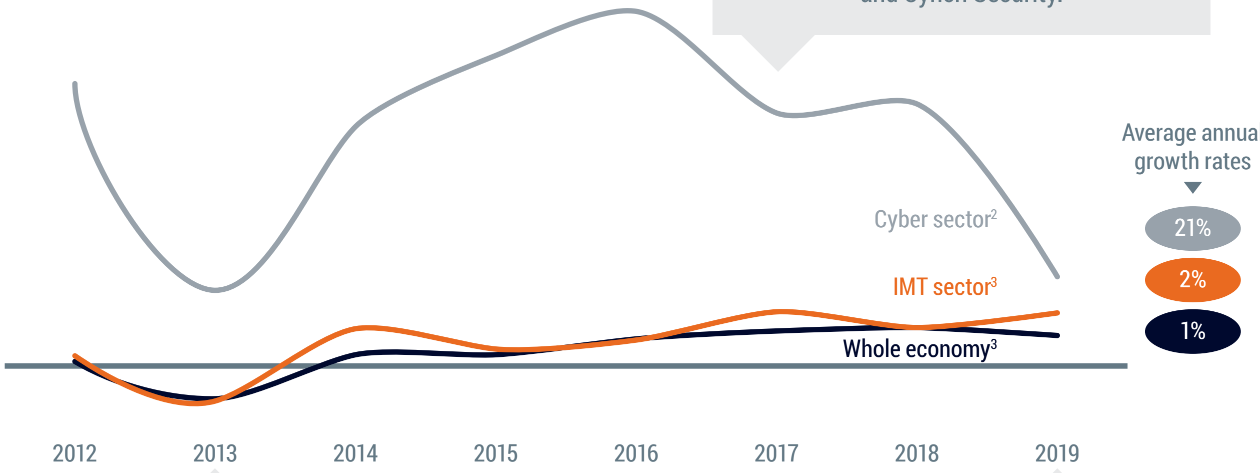
The decline in the growth rate in a number of companies throughout 2018 and 2019 may be explained in part by the Digital Census not capturing the newest companies in the sector, and by market consolidation in the formation of CyberCX and others.

Figure 29

Growth rate in number of companies by sector

Per cent per year

53 per cent of Australian cyber companies were established in 2015 or after, including Cynterra, Secure Code Warrior, Tesserent and Cynch Security.



2013 saw a drop in confidence in worldwide recovery from the global financial crisis and in China's ability to support Australia's mining boom. This reduced new company establishments across the economy.[1]

Note: Cyber sector growth in 2019 may be understated, as our survey sample may not have captured the newest companies in the sector.

1. Lim, G C Chua, C L and V H Nguyen (2013), Review of the Australian Economy 2012-13: A tale of two relativities, *Australian Economic Review*, 46(1). pp1-13
2. Survey question: When was your organisation established?
3. Australian Bureau of Statistics (2020) *8165.0 Counts of Australian Businesses, including Entries and Exits*, Jun 2011 to Jun 2015 and Jun 2015 to Jun 2019. Table 1: Businesses by Industry Division. Available at: https://www.abs.gov.au/statistics/economy/business-indicators/counts-australian-businesses-including-entries-and-exits/latest-release

However, investment in cyber startups is lower in Australia than in peer economies

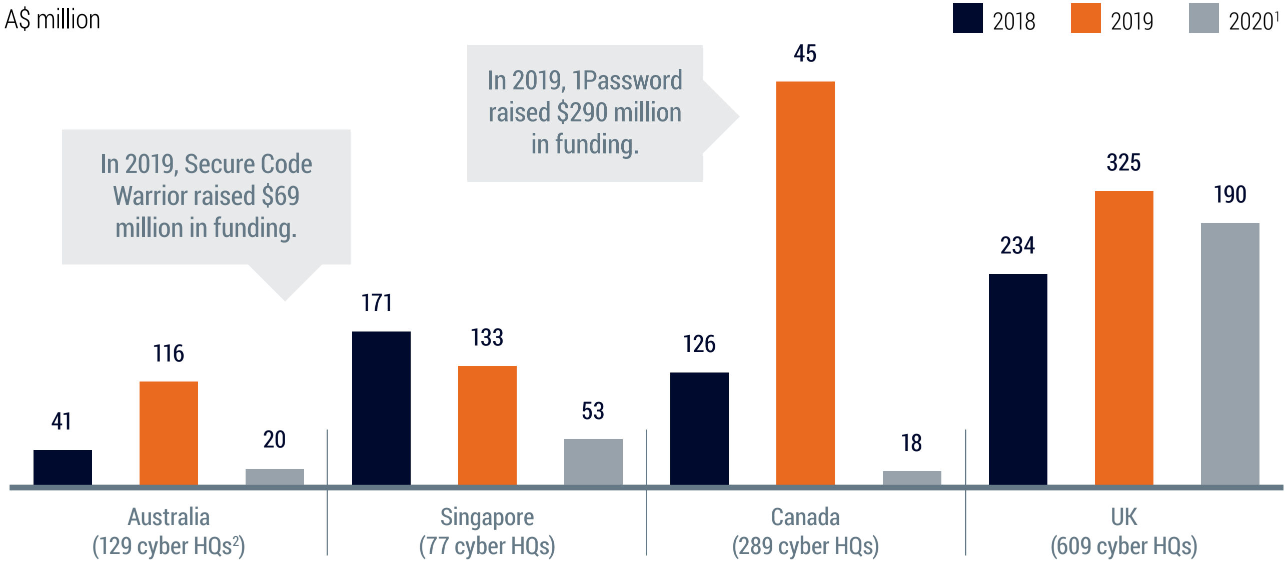
Lack of finance and investment continues to be a significant barrier to startup growth: nearly 50 per cent of survey respondents cited it as one of their top three challenges. This is borne out in the data: startups headquartered in Australia have generated less value in early-stage funding rounds in each of the last three years than those headquartered in Singapore, Canada or the UK. Two problems explain this relative underperformance:

- **Cyber startups struggle to effectively engage the venture capital (VC) community:** investors are optimistic about the cyber industry, but startups often lack the commercial and sales capabilities to communicate and demonstrate the financial viability of their solutions. This leads to less engagement with the VC community as a whole.
- **There is a lack of depth in local investment opportunities:** Australia's cyber startups have not yet generated the critical mass that would entice large funds specialising in cyber security. As a result, investors in Australia do not invest in cyber security because they cannot deploy the capital needed in Australia alone. This reinforces the need for Australian cyber providers to have a global outlook from their inception.

The overall result is that Australian cyber startups raise less capital than they need, which constrains growth and limits their ability to succeed.

Figure 30

Value of early-stage funding rounds



In 2019, Secure Code Warrior raised $69 million in funding.

In 2019, 1Password raised $290 million in funding.

Over the last three years, Australian providers raised A$177 million compared to their Singapore counterparts, which raised A$357 million, even though Australia has more startup headquarters (129 vs 77).

Note: A small portion of funding rounds did not have fundraised amounts, due to confidentiality. These rounds were counted in the total number of rounds but not in the total amount raised. Where multiple investors were listed, fundraised amounts were attributed across each investor evenly. Where no investor was listed, the average ratio of Australia (or Singapore) versus overseas was applied to the total amount of funds raised

1. 2020 includes funding rounds up to October 2020
2. This number only includes fully dedicated cyber providers who list their primary HQ in Australia, It does not include providers who offer cyber as one part of a larger offering

Sources: Crunchbase, PitchBook, AlphaBeta analysis

While Australia's cyber innovation ecosystem is growing, it could keep learning from international peers

Having a mature, entrepreneur-led innovation ecosystem is essential to ensure the sector's growth. The ecosystem provides a space where founders can meet mentors, clients and collaborators, while improving the sector's visibility and attracting more capital and customers.

There is widespread acknowledgement that although it is improving, Australia's cyber security innovation ecosystem still relies on 'everybody knowing everybody', rather than an underlying structure that can independently support growth. For example:

- While startup-to-startup collaboration is strong and there are hubs that bring together researchers, startups and customers, there are few systematic pathways for technically strong cyber founders to connect with entrepreneurs that have commercialisation skills in capital raising, sales and marketing.
- A small number of highly supportive private sector companies willingly test and validate cyber startup products and services, but broadly speaking there is a shortage of formal, low-cost ways for startups and customers to propose problems, test ideas and jointly solve challenges.

Figure 31

Cyber innovation ecosystems in peer countries

London and Cheltenham

There are clusters of cyber security startups around the UK's defence and intelligence centre in Cheltenham and supporting London's broader business and technology industries. A well-structured and robust ecosystem supports sector development through:

- **visibility** within the business community about where to go for cyber expertise or for people with startup ideas (such as the London Office for Rapid Cybersecurity Advancement);
- **regular events and meetups** that support formal and informal transfer of knowledge at all levels of the ecosystem (such as the VC-hosted London Cyber Security Meetup, and the Cyber Security Entrepreneurs & Leaders Meetup);
- **anchor providers** such as OneTrust, Darktrace, Ravelin and Snyk that pave the way for new startups; and
- **investment** in cyber security has emerged at the top of the investment agenda for the UK's leading banks[1]

[1] Lloyds Bank (2019), *Commercial Banking Financial Institutions Sentiment Survey 2019*. Available at: https://www.lloydsbankinggroup.com/Media/Press-Releases/2019-press-releases/lloyds-bank/financial-institution-2019-survey/

Figure 31

Cyber innovation ecosystems in peer countries

Montreal

Montreal's government is actively developing the city's cyber security sector. Its approach seeks to coordinate large organisations to work together through initiatives such as:

- **events** that bring members of the startup system together to share knowledge and connect with services (such as GoSec and NorthSec);
- **collaboration hubs** that connect startups to researchers, industry and investors that are looking for new products or services (such as CyberEco, the Smart Cybersecurity Network and Canada's Centre for Cyber Security); and
- **public investment and support** that is tailored to startups, including tech-friendly R&D incentives and tax credits, and public investment.

New York City

Cyber NYC is an ecosystem supporting cyber startups mostly in the banking and finance sector. It supports industry growth through education and by bringing together demand, investment finance and talent. This includes:

- **building talent** through industry and academic collaboration on undergraduate, graduate, retraining and continuing education programs;
- **catalysing innovation** through structured programs that bring together ideas, research, talent and funding (such as Moonshot Challenges and Inventors to Founder programs); and
- **meeting demand** by acting as a one-stop shop for buyers to diversify their talent pool; tap into partnership and acquisition opportunities; and find marketing and sponsorship opportunities.

> Government support for early-stage funding must better match the needs of startups

Growing the cyber security sector will require maturing research funding, the innovation ecosystem and investment opportunities

Provide ongoing support and funding for the development of cyber security research hubs that focus research efforts

- Australia has increased its funding for cyber security research to approximately $64 million over the past three years, a level that is higher than in Singapore and in Canada in absolute terms, and more than in the UK in relative terms.
- The addition of the Cyber Security CRC has improved the focus of Australia's cyber security research and provided a platform for collaboration between businesses and the research community.
- However, for Australia to continue building its cyber advantage, it will need multiple research hubs and institutions, each focused on topics of strategic and competitive strength, that can bring together industry and researchers to compete in a global innovation landscape.
- Stable government funding, along with industry support, will be essential to enable these hubs to grow and mature.

Mature the innovation ecosystem's infrastructure to provide better connectivity

- The cyber security innovation ecosystem has developed quickly over the past three years with the maturing of AustCyber's programs, the launch of dedicated cyber security accelerator CyRise, the Cyber Security CRC, and new innovation opportunities in critical infrastructure.
- Survey results also show there is some collaboration in R&D between providers, which indicates the strength of networks within the sector, but there is less evidence of collaboration between providers and customers.
- For the sector to continue growing, its innovation ecosystem must mature and make stronger connections between technical experts, entrepreneurs, investment finance and customers.
- A more mature system must help generate more opportunities for startups to test products and services with customers. Better and more frequent connections between startups and customers will ensure new products, services and innovation are customer-oriented.

Facilitate access to seed and early-stage VC through more practical policy supports and improved promotion

- Debt and equity financing is crucial for any business to build its products and services, expand its customer base and scale its business.
- While specific programs have unlocked finances, Australian startups access capital at lower rates than startups headquartered in peer economies. Interviews highlighted key barriers such as overcoming the funding gap in the seed and early-series funding stages, and in the scale-up phase.
- Government support for early-stage funding must better match the needs of startups. Examples include capital contributions, rolling grants and seed funding that allow startups to thrive outside 12-month grant application cycles, as well as low-interest loans for R&D. Traditional tax credit schemes are less helpful for startups as they often make a loss or only break even when first being established.
- In addition to increasing funding mechanisms, attracting investment in local companies requires showcasing local businesses to build depth and interest in the local market. This will also overcome hurdles for investors that are looking to find high-potential cyber investments in Australia in a highly competitive and globally mobile capital market.

3.2 MARKET MATURITY AND ACCESS

Cyber security demand is maturing

Demand for cyber security products and services is maturing in three key ways. Firstly, consumption of cyber security products and services is spreading into more sectors. Historically, heavily regulated private-sector entities in banking and utilities – and Australian Government defence and national security agencies – treated cyber security as a serious risk. Anecdotally, other sectors saw it as a box to tick within the IT portfolio. But this is changing. Awareness is spreading beyond the ASX 20 through the ASX 200 and to similarly sized private companies about the importance of strong digital protections.

Secondly, companies are better understanding the products and services they require. Across the market, new buyers are realising they need minimum protections, while more established buyers increasingly choose higher-quality products and services.

Finally, companies are increasing their depth of spending on cyber security (see Figure 32).

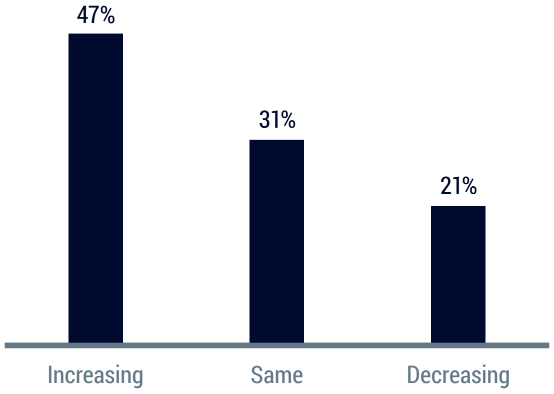
Several factors drive this maturation in demand:

- **Businesses' own digitisation:** as businesses digitise their own products and services and adopt more back-of-house technology, they increasingly realise the threats they can be exposed to.
- **Government regulation:** the Australian Government and other industry regulators are mandating stricter minimum cyber security requirements. Globally, this is widely acknowledged as a key driver of demand. Examples include the USA Health Information Privacy Act (HIPA) and National Institute of Standards and Technology (NIST) regulations; the EU General Data Protection Regulation (GDPR); and other breach notification or minimum standard regulations in California, Singapore, Vietnam and the United Arab Emirates. Australian milestones include:
  - the Australian Government's 2020 consultation around expanding Critical Infrastructure and Systems of National Significance regulations in 2021;
  - the Australian Prudential Regulation Authority (APRA) providing cyber security prudential guidance in 2010 before legislating minimum standards in 2019;
  - the Australian Energy Market Operator (AEMO) adopting the Australian Energy Sector Cyber Security Framework in 2018; and
  - the Australian Government's data privacy breach notification laws, introduced in 2018.
- **Broader awareness-raising events:** other public events such as the Prime Minister's speeches in 2020 about the rising cyber threat from cybercriminals or malicious state actors; media reporting of significant cyber security incidents at large companies; and more targeted initiatives such as the Australian Cyber Collaboration Centre's briefings and simulation programs for board members, the C-suite and executives.[1]

Cyber providers still express some frustration with the maturity of demand, ranking it the biggest challenge facing the sector. While it may still have some way to go, the factors driving maturity are only likely to increase as businesses transform their operating models and governments regulate to ensure confidence in the resilience of the economy.

Figure 32

Forecast cyber security budget changes FY2021–22



- Given the year that 2020 was, with many security executives not having certainty for their FY2020–21 budgets until much later than they are used to, it is encouraging to see that there is optimism for the future.
- 47 per cent are expecting that their FY2021–22 budget will increase from FY2020–21.
- 31 per cent expect their budget to hold steady.
- The COVID-19 pandemic and the second and third order effects are still to be seen.

Source: Percentages have been rounded and will not equal 100 per cent. For full analysis, see the *CISO Lens Benchmark 2020*. Available at: https://www.cisolens.com/

[1] Prime Minister of Australia's office (2020), *Statement on malicious cyber activity against Australian networks, Australia's 2020 cyber security strategy.* Available at: https://www.pm.gov.au/media/statement-malicious-cyber-activity-against-australian-networks

Collaboration between Australian providers is an effective way to boost competitiveness

Australian cyber security is developing a rich network of collaboration, particularly in product and service delivery, and commercial functions such as marketing.

Examples of collaboration include:

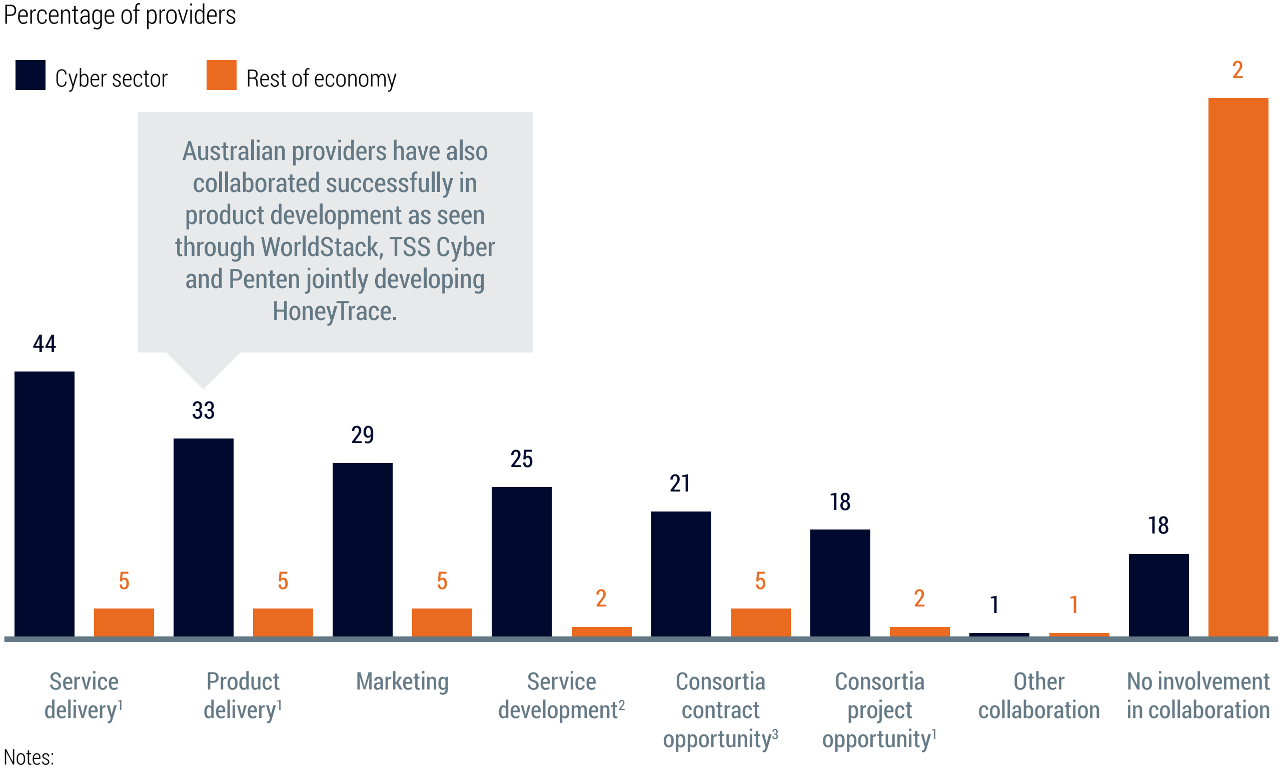
- **vertical collaboration** where cyber security providers like Kasada build offerings on top of technology platforms like Amazon's cloud systems; and
- **horizontal collaboration** between providers that have complementary capabilities and can offer a more holistic solution to customers.

Around 44 per cent of providers work together for service delivery and around 33 per cent partner on product delivery. Around 29 per cent of organisations in the sector work together to save on commercial functions, such as marketing.

This collaboration is characteristic of a sector that is growing quickly and in the process of consolidating and scaling. Collaboration can be a viable strategy for startups to initially add capabilities, save on costs, access more customers and compete in the broader market. However, as the sector matures and successful startups consolidate, this level of collaboration may no longer be necessary and could decrease.

Figure 33

Collaborative arrangements in Australia's cyber sector vs the rest of the economy



Notes:

1. For the economy-wide result, 'Service delivery', 'Product delivery' and 'Consortia project opportunity' are proxied with 'Joint production of goods and services'
2. For the economy-wide result, 'Service development' is proxied with 'Integrated supply chains'
3. For the economy-wide result, 'Consortia contract opportunity' is proxied with 'Joint buying'

Survey question: Was your organisation involved in any collaborative arrangements during FY20? If so, what kind?

Sources: AustCyber's Digital Census 2020. Australian Bureau of Statistics (2020), *8167.0 Characteristics of Australian Business, 2018-19: Business collaboration* Available at: https://www.abs.gov.au/statistics/industry/technology-and-innovation/characteristics-australian-business/latest-release

However, government procurement remains a significant challenge for younger and smaller providers

Government procurement is widely recognised as a fast-acting, high-impact lever for driving sector growth. However, the Australian Government and state and territory governments continue to make conservative procurement choices that discourage competition and lock out new providers. For example, they often:

- adopt exclusive tendering approaches such as panels, which are not transparent regarding the type of problem being addressed;
- have complex and resource-intensive requirements for participation in tenders, including a heavy compliance and paperwork burden;
- limit market information and competition by withholding the prices and details of contracts awarded; and
- enforce expensive or time-consuming accreditation processes for the products and services of SMEs.

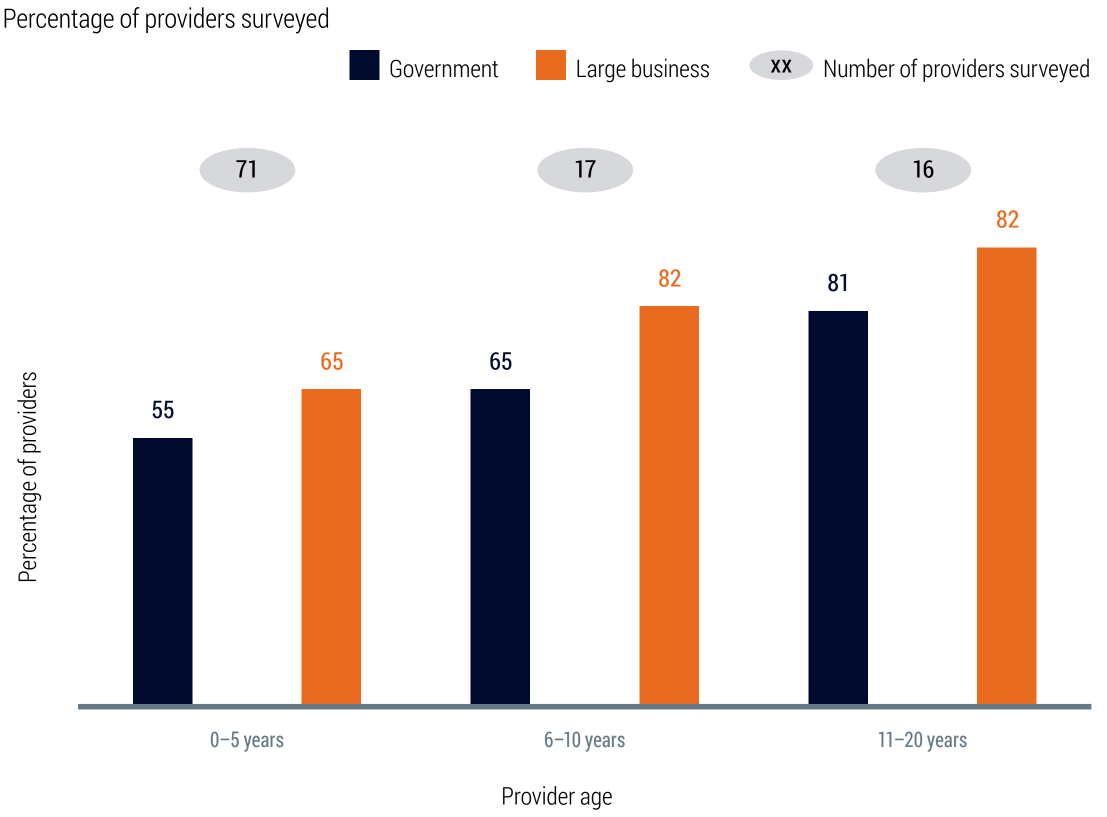
These policies hamstring local sector growth: only 55 per cent of providers aged between zero and five years are selling to the Australian Government or state or territory governments, compared to 81 per cent of providers aged between 11 and 20 years. This pattern is largely reflected when comparing providers by size: less than 60 per cent of providers with fewer than 20 employees are selling to the Australian Government or state or territory governments, compared to more than 80 per cent of providers with more than 20 people.

Australian governments recognise this, and are beginning to create opportunities for the local sector. Initiatives such as the NSW ICT/Digital Sovereign Procurement Taskforce and AustCyber's GovPitch are designed to facilitate the entry of Australian providers into supplying the public service. However, cyber providers must also play their part by adapting their offerings and proving their value to many governments that are justifiably risk-averse in their buying behaviours.

Procurement by large businesses is comparatively easier, and more providers count large businesses as their customers. However, younger and smaller cyber providers still sell less to large businesses than bigger and more established providers do.

Figure 34

Percentage of providers selling to government and large businesses



Note: Results are only representative of providers that responded to the survey. Large businesses are defined as organisations with more than 200 employees. Government includes state and territory governments, and the Australian Government
Survey question: Did your organisation provide cyber security products and/or services to any of the following customer groups in the last 12 months?
Source: AustCyber's Digital Census 2020

CASE STUDY

Building a single brand to showcase shared systems and a united mission

CyberCX has sought to provide local customers an Australian alternative to large multinational providers for complex cyber security services.

Launched in October 2019 and backed by private equity firm BGH Capital, CyberCX has brought together 15 (and counting) independent cyber security service providers over the course of the past year. Some of these providers are well known Australian names – including Shearwater, CQR, Sense of Security, TSS and Phriendly Phishing.

CyberCX's approach to scaling – by acquiring and consolidating existing providers who have proven capabilities and prior customer bases – means the organisation has been able to develop into a large and competitive provider within a short period of time.

CEO John Paitaridis said, "CyberCX took a structured and deliberate approach to integrate its group of portfolio companies into a single organisation, building shared systems and a united mission, under a single brand".

CyberCX's acquisitions reflect an ambition to unite a complementary set of cyber services. As recently as October this year, CyberCX acquired the publicly listed Cloudten and Decipher Works – who specialise in cloud and identity management, respectively – to meet growing demand around cloud services driven by the COVID-19 pandemic.

"COVID-19 has accelerated enterprises' cloud migration strategies and highlighted the need for robust identity management solutions," said Mr Paitaridis[1].

Chief Strategy Officer Alastair MacGibbon has signalled that CyberCX will continue to scale further by expanding overseas in 2021. He said, "CyberCX plans to significantly grow our specialised cyber security workforce across the UK and US to deliver end-to-end cyber security services".

One of CyberCX's earliest acquisitions (CQR) had an existing presence across the UK which will help CyberCX scale its presence overseas. The organisation plans to double its cyber security workforce across New Zealand, the UK and US in the next year in an attempt to create a large, globally competitive, Australian cyber services alternative.

[1] ARN (20 October 2020), *CyberCX forks over $25M to buy Cloudten and Decipher Works*

CyberCX

Although export performance is very promising for a young sector, cultivating clearer channels to market will help providers compete internationally

Cyber security is an inherently global sector. Because the threat landscape transcends national borders, so do the technological cyber security products and services that protect against those threats. Investment finance and the competitive landscape are also international for these reasons. In a world where threats and competition for cyber protection are global, Australia's sovereign capabilities must be equal to the best in the world.

A promising share (43 per cent) of businesses in Australia's young cyber security sector are already exporting, and the average revenue from exports across all SME cyber providers is around 15 per cent.

Australia's reputation as a highly capable, trustworthy and cost-competitive exporter is a key strength and trade enabler.

The most significant barrier to export is Australia's channels to market. Because Australia's strength is in services, accessing buyers relies on relationships and word of mouth much more than trade fairs. Local businesses need strong credentials and first-reference customers. Government also has a role to play in connecting local businesses to international buyers by leveraging its relationships with other governments and large businesses.

Figure 35

Status of key export enablers

Key ⬛ Strength 🟧 Neutral ▨ Weakness

Trade enabler	Status	Explanation
Global outlook	🟧	- Some cyber businesses recognise the need for global perspective and scale; others are focused on local customers. - Maintaining and growing this global outlook will help startups better understand their competitive environment.
Reputation	⬛	- Australian businesses share a reputation as trusted business partners; Australian cyber providers are seen to be competitive on quality and cost compared to other imports in key markets. - Leveraging this reputation should be a key export tactic.
Local partnerships	🟧	- There is a strong, but small, number of partnerships in defence supply chains and some key regulated markets. - Replicating these high-quality partnerships into new customer groups will help grow exports. - Efforts should be focused on in-market partnerships with larger cyber providers such as MSSPs, as well as tech providers such as AWS and Microsoft.
Channels to market	▨	- Channels to market for Australian providers are the weakest trade enabler. Services exports take stronger relationships to facilitate than products, and key supporters such as governments and defence primes are not optimally leveraging their connections.
Flexibility	🟧	- Some startups struggle to understand and adapt to other countries' business norms, although export playbooks by Austrade and AustCyber are helping. - Better flexibility and export-readiness will lead to more successful trade and international competitiveness.

Australia's cyber businesses need a competitive marketplace and support to scale and become globally competitive

Maintain and strengthen the sector's global, export-oriented outlook

- The Australian sector already has a strong export orientation: 43 per cent of businesses are already exporting and there are trade links across most key markets.
- Support for companies looking to go global through trade delegations, market research publications, training and introductions to customers has been critical to the success of Australian companies abroad.
- Maintaining this support in target markets will be vital to the future of Australia's cyber security sector as a globally competitive and world-leading sector. Leveraging government-to-government connections and supporting Australian producers with international standards information and accreditation are two examples of ways to support the global outlook of Australia's cyber security sector.

Support businesses in the sector to mature and scale

- Over the past five years, the cyber security sector has boomed: 40 per cent of Australian cyber companies have been born since then, and 66 per cent in the last 10 years. The innovation ecosystem is growing.
- Collaboration in the sector is very high: between 33 per cent and 44 per cent of startups collaborate on product and service delivery; and 29 per cent collaborate to save on back-of-house costs like marketing. This is a valid strategy for startups and SMEs to compete in a sector dominated by large providers while they are still young and establishing.
- The next stage of development for cyber security providers is to consolidate and scale so they can become mid-tier and large businesses capable of competing with global providers. Two particularly promising opportunities are horizontal mergers between businesses with complementary skills, and vertical integration into technology alliances or through supply chains via secure by design.

Improve the openness and competitiveness of government procurement processes

- More open and competitive procurement systems will allow local cyber companies to bid competitively and unlock more contracts.
- While programs such as GovPitch and facilitated offshore business delegations have helped connect some providers with buyers, difficulty securing government and large business customers remains a large barrier for small businesses.
- Several practical improvements to procurement processes could enhance competition and result in better quality and/or lower-cost products and services. These improvements could include:
  - exempting new providers and technology companies from anti-competitive panel requirements;
  - increasing market information and competition by publicly publishing prices and details of contracts awarded; and
  - increasing fairness of contract terms, including better intellectual property protections and more flexible pricing and commercial conditions.

Support data, privacy and other regulations that bring security and trust to the digital economy

- The regulatory environment has evolved significantly over the past five years, with notifiable data breaches, encryption legislation and recent announcements on standards and critical infrastructure.
- Continuing to regulate cyber security will help to maintain trust and confidence in Australia's digital infrastructure and businesses. Regulation helps mature demand and will increase the customer base for Australian cyber solutions. Consultation and co-design with industry and international partners is critical to support global competitiveness and assure the innovation that helps all organisations push back on malicious cyber actors.
- One area where Australia's regulation is particularly underdeveloped is cyber insurance, which can help manage cyber risk and encourage investments in cyber security.

3.3 SKILLS AND WORKFORCE

Since 2018, there has been a sharp increase in cyber security-specific training programs across Australia

Australia's tertiary education system plays a pivotal role in enabling the continued growth of the cyber security sector. Due to its rapid expansion, the sector has historically faced a talent shortage. However, Australian TAFEs and universities are mobilising to address this skills gap, with half of all Australian universities now offering cyber security as a specific degree or a major in information technology (IT) or computer science qualifications. The benefits will take time to flow through to providers, but there are positive signs, with more than 50 per cent of cyber providers surveyed being more confident about the talent pipeline than they were five years ago.

Importantly, there are now over 20 dedicated postgraduate programs (including graduate certificates and graduate diplomas) targeting people who may already have experience in IT or related fields. This is significant as interviews suggest that many Australian cyber security providers experience a shortage of talent at the more senior levels.

Although the rising number of cyber-specific programs is promising, it is vital that student interest in cyber security meets this growing supply. As such, securing the talent pipeline needs to begin in primary and secondary schools. Schools have an important role to play in educating our young people in cyber security skills, and exposing them to the possibility of an exciting career in cyber security. School-level initiatives to grow this interest have also expanded in recent years (see Figure 36).

Figure 36

Cyber security presence in tertiary education

Pre-2014

ECU Edith Cowan University; UNSW Australia

Foundations

In 2001, Edith Cowan University launches one of the first dedicated cyber security courses in Australia.

In 2013-14, the University of New South Wales develops a postgraduate program in cyber warfare and in 2015 pioneers and launches a novel education partnership with the Commonwealth Bank worth $1.6 million.

2014–17

La Trobe University; Macquarie University; Box Hill Institute; Charles Sturt University; University of South Australia; Canberra Institute of Technology

Early support

Tertiary educators begin turning to the private sector for joint investment in training, with Optus co-funding a market-leading cyber security degree at La Trobe University in 2016.

Box Hill Institute collaborates with industry to develop the Certificate IV in Cyber Security.

2018–19

The University of Adelaide; Western Sydney University; Deakin University; QUT; Australian National University; TAFEcyber; RMIT University; Curtin University

Institutions mobilising

More than ten institutions begin offering cyber security-specific programs as TAFEs around Australia start teaching Certificate IV in Cyber Security.

Deakin University recognises the Certificate IV in Cyber Security as prior learning for its cyber security courses.

Other major universities review their curriculum to include cyber security in non technical course offerings.

2020+

FifthDomain Securing Cyber Skills; Cyber Aware; CyberCX; With You With Me; Ionize

Continued growth

As demand for cyber security professionals continues to increase, institutions are rising to the challenge with more than 20 universities now offering cyber security as a specific degree or a major in IT or computer science.

Continued numbers of private entities offering quality cyber security skilling opportunities.

Note: Displayed educational institutions are not exhaustive.
Source: Victorian Skills Gateway, AlphaBeta analysis of cyber security higher education offerings, expert interviews

The increasing availability of cyber security courses and qualifications in the university and vocational education and training (VET) systems is reflected in dramatic growth in course enrolments.

In just a few years, VET enrolments in cyber courses have increased from less than 500 students to around 3,800 in 2019. More than two-thirds of these students are studying at Certificate IV level, with the remainder undertaking a diploma or advanced diploma. Enrolments in undergraduate and postgraduate university courses have also grown rapidly.

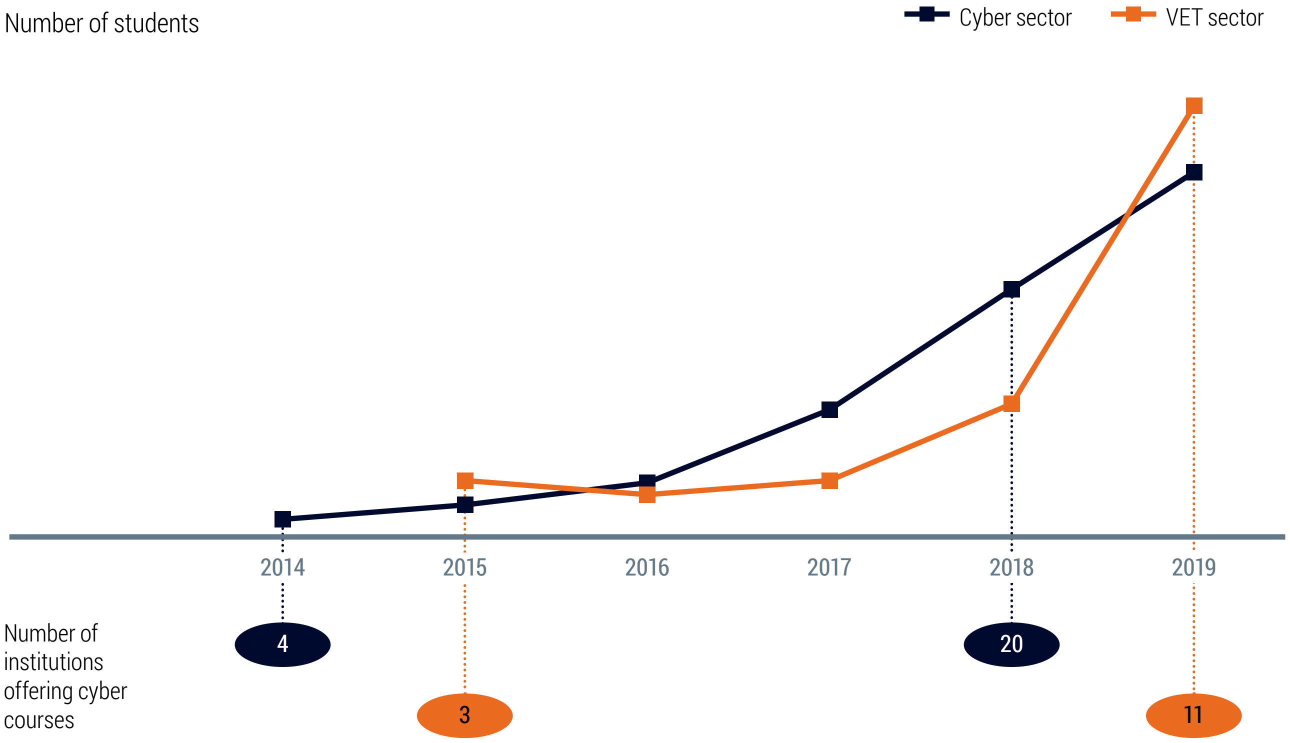
Collaborative, industry-led programs have been key to this development, especially in the VET sector. Below are some major VET initiatives:

- In 2018, Box Hill Institute developed two cyber security training products, funded by industry and supported by AustCyber, and launched the TAFECyber Initiative.
- In 2020, the AustCyber Projects Fund was used to extend the work of the TAFECyber Consortium of ten TAFE colleges, to coordinate learning resources, training product development and professional development for educators.
- Also in 2020, TAFE NSW and the NSW Cyber Security Innovation Node, supported by Hewlett Packard Enterprise, launched cyber security mini-modules online to help workers retrain through COVID-19.

While the growth in enrolments has been impressive, maintaining this momentum will be vital. The workforce is forecast to grow by 7,000 workers over the next four years and, factoring in natural attrition, the number of new workers required is likely to be closer to 10,000.

Figure 37

Enrolments in cyber-specific VET and university courses



Note: VET system data only includes courses with ‘cyber’ in the title; VET ‘courses on offer’ includes both courses *and* skill sets (two skill sets were introduced in 2019), but institutions offering courses do not include skill sets, and there is no associated enrolment data to identify which registered training organisations deliver the training.

Sources: NCVER DataBuilder (2020), *Total VET students and courses: course enrolments*, Department of Education, Skills and Employment, University Statistics Section data request (2020), Student enrolments in cyber security, My Skills (2020), *Training Provider Search*

CASE STUDY

Building awareness in the classroom to enable the cyber workforce of the future, today

Understanding how our digital world works, how it is designed to protect us and how we can keep our information safe is critical for both adults and children to learn.

The University of Adelaide (UoA)'s Computer Science Education Research Group (CSER Group) have been operating digital technologies programs for Australian teachers since 2014.

"The entire CSER program, which includes eight MOOCs on various technology curriculum related areas, has attracted over 38,000 enrolments," said Dr Rebecca Vivian, CSER Project Lead.

This year, they partnered with AustCyber, CSIRO and Google Australia to develop free, self-paced Massive Open Online Courses (MOOCs) to build primary and secondary teachers' confidence and capacity to integrate the learning of cyber security and awareness into the classroom.

Two new courses – one for primary teachers (K-6) and one for secondary teachers (years 7-10) – contain practical classroom activity ideas and examples of career pathways. Both courses are aligned to the Australian Curriculum (Digital Technologies and ICT Capabilities) and focus areas include data security, encryption, cryptography, networks, information systems and safety, cyber security risks and security measures, and cyber ethics.

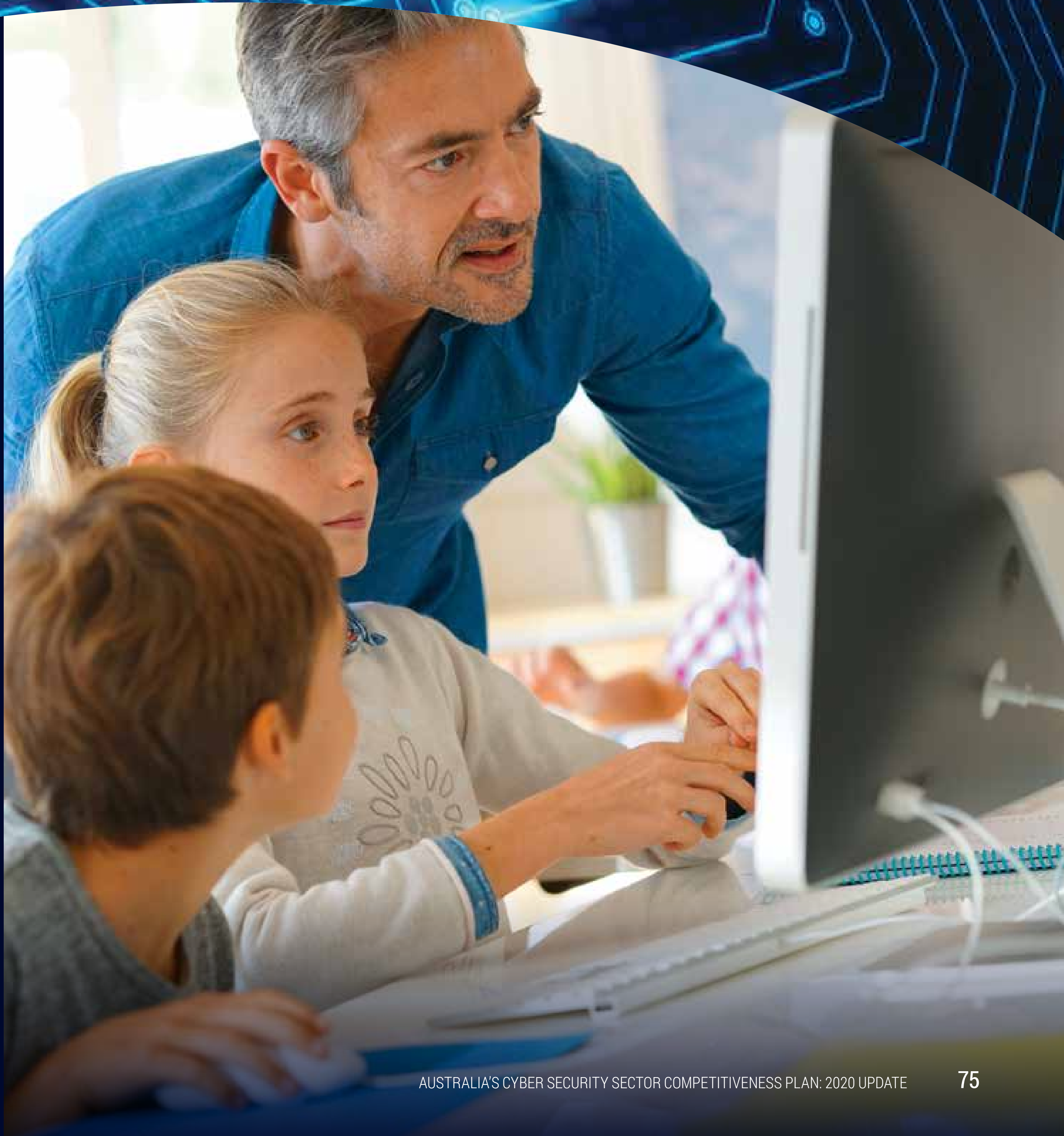
"The Cyber Security and Awareness MOOCs for Primary and Secondary Classrooms have been live since mid 2020, with over 770 teachers enrolled to date," said Dr Vivian. "Given there are over 288,000 teachers in Australia, we have many more to reach. Learning about cyber security not only enables students to adopt safe practices in their own use of technology, but importantly, can inspire a future cyber security workforce."

In today's digital world where children are exposed to social media and they consume large amounts of online content at an early age, the need for early and relevant cyber education is crucial. The UoA's MOOCs are an important tool for building cyber awareness. Nurturing cyber literacy amongst school students also helps grow the sector's talent pipeline by highlighting the various pathways available to students.

THE UNIVERSITY *of* ADELAIDE

Over the past three years, there has been significant progress in the availability of cyber security courses and training. This momentum needs to continue to meet the growing demand for cyber security professionals, with the workforce estimated to increase to 33,500 by 2024.

Primary and secondary schools play a crucial role in ensuring this demand is met. If schools can encourage students to consider a career in cyber security, while also building early cyber skills, both the quality and number of students looking to undertake cyber security qualifications will improve.



> Although the rising number of cyber-specific programs is promising, it is vital that student interest in cyber security meets this growing supply

New training programs and the upcoming launch of Cyberseek Australia ensures key enablers are in place to transition workers

Figure 38

Key enablers to transition workers into the cyber security sector

1. Transferring skills

Are there workers with relevant skills in adjacent industries?

There is a continuing strong supply of high-potential workers with significant skills crossover.

Transferable skills include:

- IT architecture, IT support, risk monitoring, software programming, application testing, data and pattern analytics, user testing, user experience, project management, strategy development, policy, law, investigations.

Adjacent sectors include:

- software development;
- systems engineering;
- financial and risk analysis;
- networking; and
- security intelligence.

2. Attracting talent

Is it attractive for workers to transition from other sectors into cyber security?

Expert interviews suggest that cyber security workers continue to receive a significant wage premium over their IT counterparts.

However, information about cyber security workforce opportunities has been more limited. In early 2021, a new market information tool called **Cyberseek Australia** will launch with support from AustCyber. It will provide information on:

- cyber skills demand by region across Australia;
- qualification and certification requirements for cyber roles;
- indicative salaries; and
- transition pathways and role progression.

3. Retraining at speed

Are there clear and accessible pathways to quickly retrain and upskill workers?

The availability and quality of transition programs has significantly increased across Australia over the past few years.

Short-term programs include:

- **17 Australian universities** offering six-month graduate certificates in cyber security;
- **11 Australian TAFEs** offering a 12-month Certificate IV in Cyber Security;
- independent providers, such as WithYouWithMe and Soldier On, offering training courses to help transition veterans into cyber security; and
- providers such as SANS, Cisco and the Australian Computer Society offering microcredentials in cyber security, which is a flexible option for rapidly upskilling in cyber.

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

The US National Initiative of Cyber Security Education (NICE), led by the US Department of Commerce, is a partnership between government, academia and the private sector that seeks to improve the America's cyber security education, training, and professional development.[1] The NICE program could serve as an example for Australia, which has yet to implement a comprehensive set of definitions to classify its cyber security workforce.

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

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

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

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

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

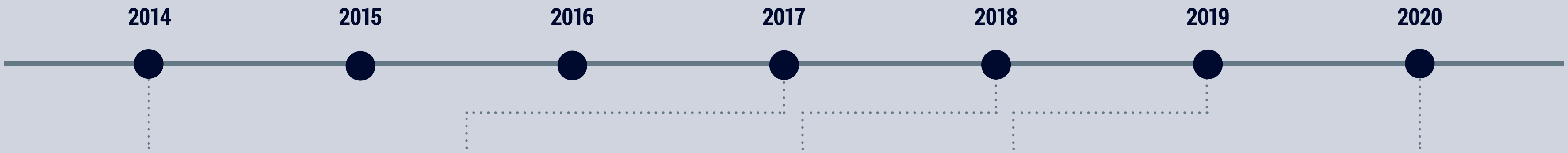
These categories are further divided into 32 specialty areas, 52 work roles and hundreds of tasks, skills, knowledge and abilities.

[1] Source: National Initiative for Cybersecurity Education (NICE). *NICE Cybersecurity Workforce Framework*. Available at: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

Cyber security teaching and resources are increasingly accessible to secondary school students

Figure 39

Timeline of cyber security programs in schools



Australian Curriculum

Digital technologies is included in the Australian Curriculum, with specific cyber safety elements available for senior years.

National Computer Science School (NCSS)

The NCSS introduces the Australian Signals Directorate-developed, cyber security-based information and communications technology (ICT) masterclass in its Summer School program.

CyberTaipan

CyberTaipan online competition is launched and reaches thousands of students across Australia in its first three years.

Kids SecuriDay is launched, running cyber security awareness workshops and events in primary and secondary schools.

Schools Cyber Security Challenges

The Australian Computing Academy (University of Sydney), AustCyber, ANZ, NAB, Commonwealth Bank, Westpac and BT collaborate to deliver the first cyber security challenge to 30,000 high school students in the first year of operations and 700,000 students in the second year. This program has now expanded to Years 5 and 6 in 2020 and the Australian Signals Directorate (ASD) is a new partner.

Dedicated cyber study camps

Data61 and the Defence Science and Technology Group at the Department of Defence plan a dedicated Cyber Security Summer School to rapidly accelerate skills, but it is postponed due to COVID-19.

Providers in NSW and Victoria are confident they can hire the workers they need, but those in other states are less positive

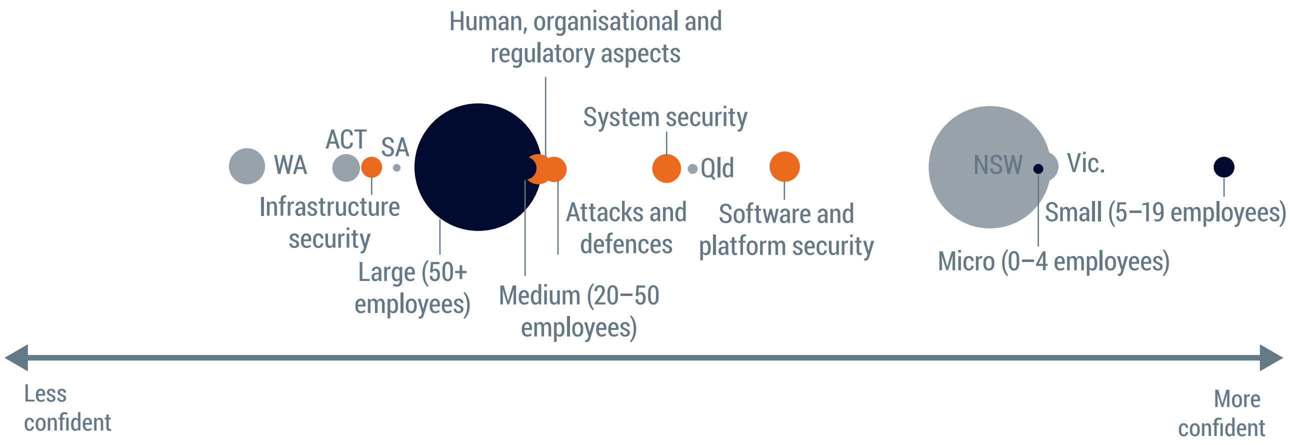
Overall, most providers report that they have more confidence in the skills system and their ability to hire the workers they need compared to five years ago.

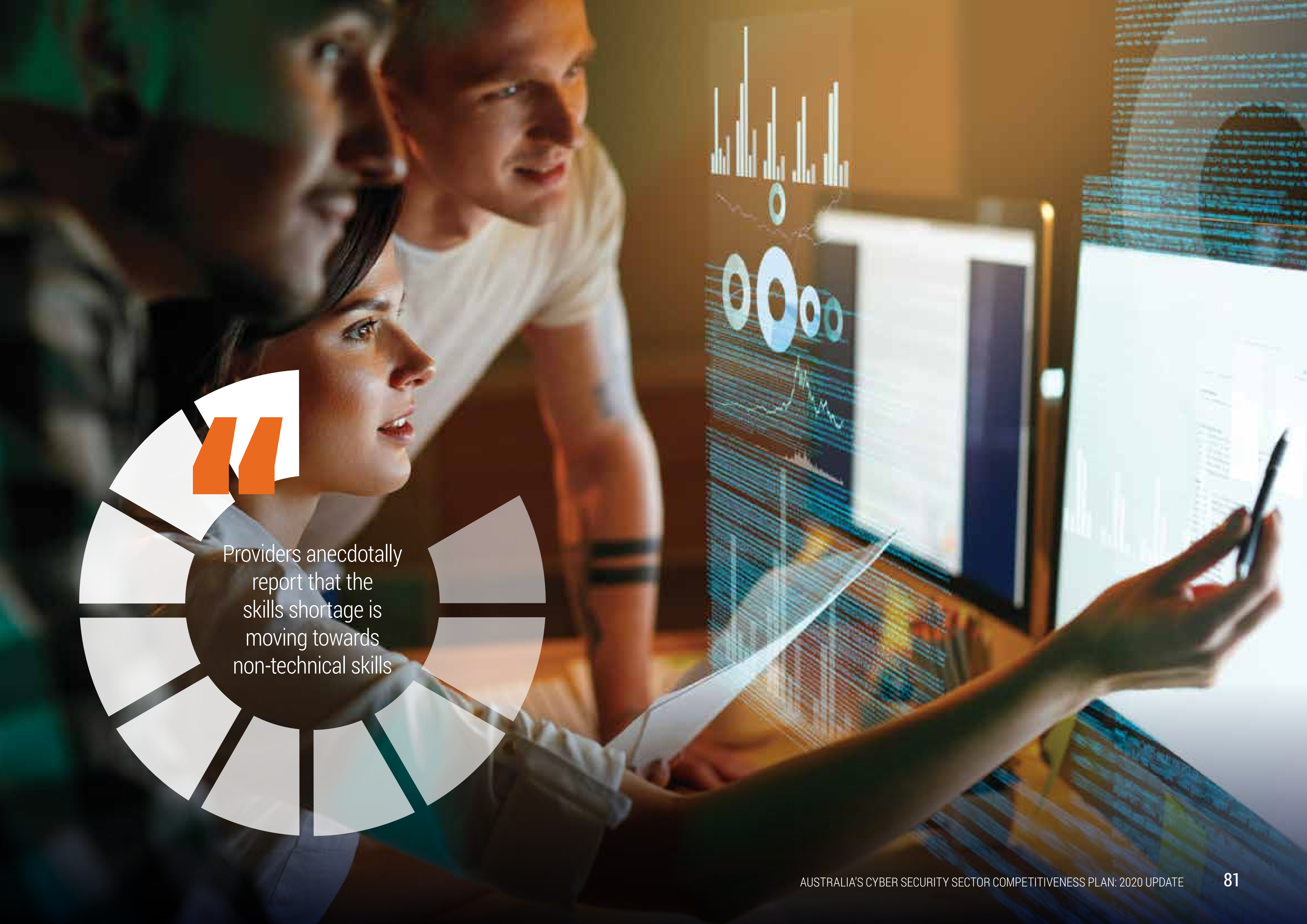
Survey data shows that providers in NSW and Victoria feel more confident compared to providers in other states, and small providers are more confident than large ones.

Providers anecdotally report that the skills shortage is moving towards non technical skills. These include leadership skills; communication skills, especially in relation to helping providers get through to corporate boards and the C-suite; and commercial skills such as marketing and operations. The latter is especially valued among startups.

Figure 40

Provider confidence in ability to access skills they need compared to five years ago





“

Providers anecdotally report that the skills shortage is moving towards non-technical skills

Much more can be done to improve diversity and inclusion in the cyber workforce

The Australian cyber security workforce is roughly 73 per cent male and 27 per cent female. Anecdotally, the gender distribution in the sector has improved over the past five years, but interviewees and survey respondents still point to an unequal education pipeline, and cultural and workplace issues that act as barriers to a more diverse and inclusive workforce.

Having a more diverse and inclusive workforce brings many benefits. At a company level, diversity and inclusion is associated with higher revenue, a greater ability to attract and retain staff, and an enhanced reputation. Sector-wide, it is correlated with higher productivity and growth, and resilience to economic downturns. Companies that are more inclusive are more competitive. Additionally, anecdotal evidence shows they have been more resilient to COVID-19's negative effects and more capable of capturing its opportunities.

Below are ways to improve the diversity and inclusion of the cyber security workforce:

- Talk about cyber security in a more accessible way: cyber security is a critical enabler for the economy, but much of the conversation around it relies on jargon that a layperson may find hard to understand. This contributes to unhelpful stereotypes of the sector such as 'hackers in hoodies' who work alone in dark rooms. The reality is that modern cyber security is a whole-of-economy endeavour that relies on a broad range of skill sets.
- Give women leaders in cyber security a platform: making the presence of women leaders in the sector more prominent will help promote cyber security as a career to more women.
- Support and connect women in the cyber security workforce: making concerted efforts to support women entering or already in the industry by facilitating networking, mentoring and community-building opportunities will help to grow the female cyber security workforce.
- Broaden outreach efforts to discover talent: facilitating work experience (for example, by providing secondary school and tertiary work experience, internships and apprenticeships) for a wide variety of potential workers who are not in computer science will attract interest in entering the sector among a more diverse range of people. Work experience opportunities can help to bridge the gap for under-represented groups, increasing participation among people of different ages, genders and neurodiversity, and First Nations people.
- Ensuring recruitment and workforce development processes are relevant and effective: implementing recruitment models that seek talent in under-represented groups, improving business cultures, and directing the attention of leaders to diversity issues will help the sector find talented workers who are currently overlooked.

Survey questions: What was the demographic make-up of your workforce in FY20? Please describe how AustCyber can assist the sector to boost women's participation in the cyber security workforce?
Sources: AustCyber's Digital Census 2020. Australian Government, Workforce Gender Equality Agency (2018), *The Business Case for Gender Equality.* Available at: https://www.wgea.gov.au/topics/workplace-gender-equality/the-business-case

Figure 41

Average female staff by company age, 2020

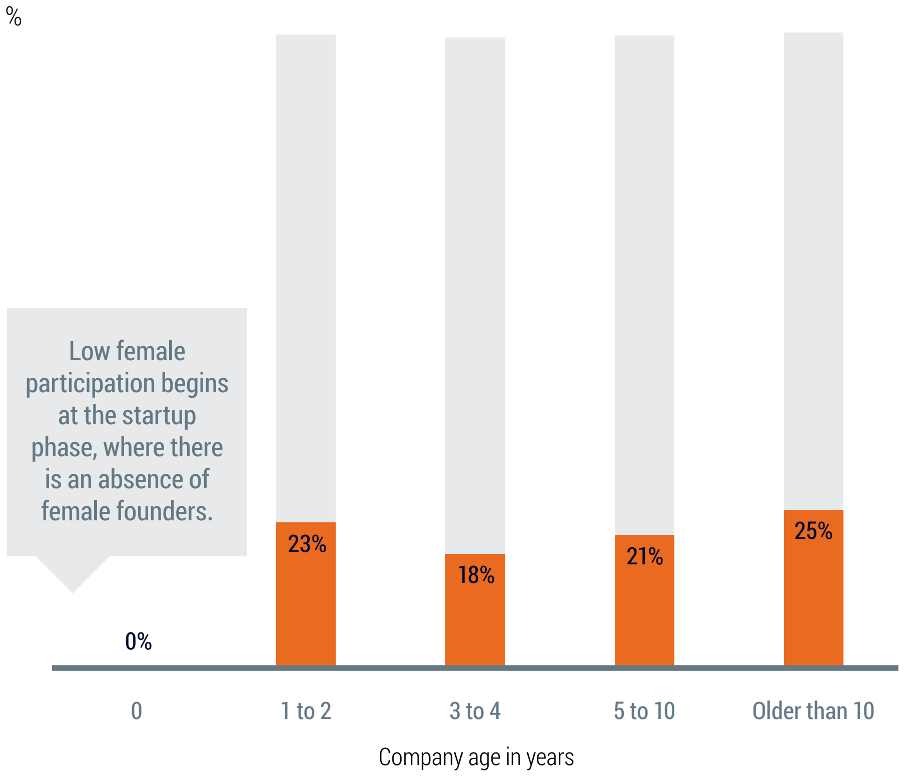
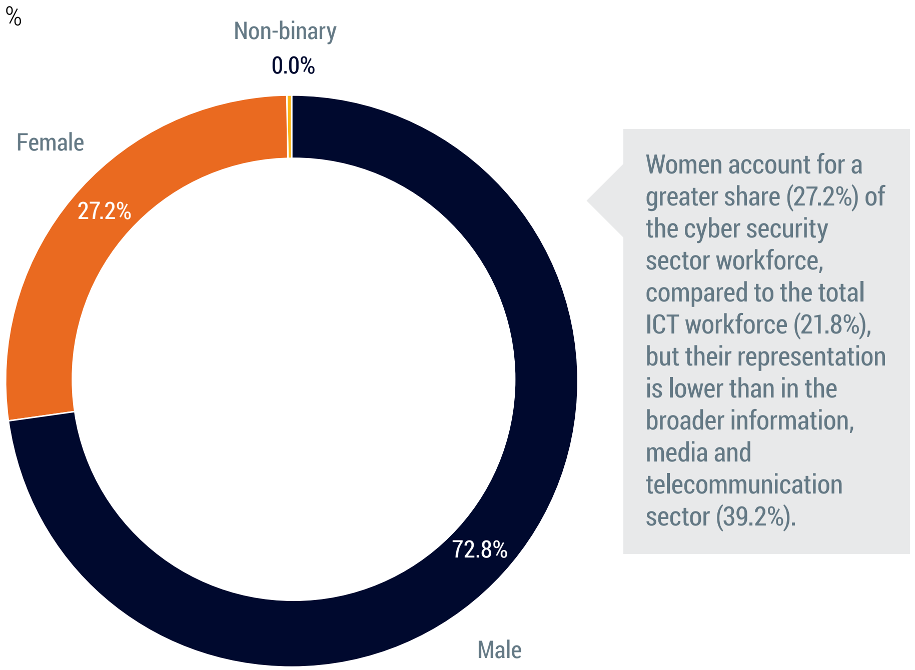


Figure 42

Cyber security workforce by gender, 2020



Women account for a greater share (27.2%) of the cyber security sector workforce, compared to the total ICT workforce (21.8%), but their representation is lower than in the broader information, media and telecommunication sector (39.2%).

Survey question: What was the demographic make-up of your workforce in FY20?
Sources: AustCyber's Digital Census 2020. Australian Bureau of Statistics (2020), *Labour Force Survey, Quarterly, August 2020*, Table 06, Information, Media & Telecommunications sector; EQ08 for following Australian and New Zealand Standard Classification of Occupations' four-digit occupations: 1351, 2232, 2252, 2600, 2610, 2611, 2612, 2613, 2621, 2630, 2631, 2632, 3100, 3130, 3131, 6212. Available at: https://www.abs.gov.au/statistics/labour/employment-and-unemployment/labour-force-australia-detailed/aug-2020

"The workforce is estimated to increase to 33,500 by 2024

Growing and diversifying Australia's cyber security talent pipeline and upskilling our leaders will ensure a strong sector and economy

Maintain momentum on growing the cyber security skills pipeline

- Over the past three years, the availability of cyber security courses and training has significantly grown, and programs to attract top talent and create vibrant professional development pathways have dramatically expanded the cyber talent pipeline. The introduction of the VET curriculum has been a significant milestone for cyber security skills in Australia.
- However, the pipeline needs to continue to expand to meet the sector's – and the economy's – growth needs. The workforce is estimated to increase to 33,500 by 2024, with around 7,000 workers requiring training over the next four years.
- Maintaining and broadening efforts to attract and train workers in cyber security expertise will ensure the future quality of Australia's cyber workforce, especially as the short-term supply of skilled migrants will be limited due to the COVID-19 pandemic.

Lift the cyber security literacy of our leaders and the broader technology workforce

- While the skills base of the sector has measurably improved in recent years, the next phase of cyber skills development requires training to improve the cyber security literacy of leaders and all technology workers.
- Improving the cyber security literacy of leaders across business, government and the community will ensure an appropriate understanding of cyber security risks and related key behaviours. The Australian Institute of Company Directors' efforts to educate directors has demonstrated how this can be undertaken.
- The Skills for Australia program, run by PwC Australia, has created cross-disciplinary VET units that have produced curriculum tools to lift knowledge. These units need to be placed in VET programs, and universities need to make similar efforts to provide cross-disciplinary cyber units of study across technology and related courses.
- Further educating all business leaders and technology workers in cyber security and emerging technologies such as AI and quantum computing is vitally important for securing Australia's digital future.

Transform the workforce to capture the benefits of diversity and inclusion

- While the workforce has rapidly grown, diversity remains a persistent challenge, with women comprising around one-quarter of the cyber security workforce.
- Accelerating the presence of female, non-binary, neurodiverse and First Nations people's expertise in cyber security will help to plug workforce shortfalls and ensure the best and brightest take up opportunities in the sector.
- Initiatives to support women entering and already in the industry are vital. Encouraging and incentivising women to pursue cyber security training will boost the pipeline of female talent. Leaders within the sector should also prioritise growing their pipelines of talent by making them more diverse.

4

THE ROLE OF AUSTCYBER

AustCyber's mission is to grow a vibrant and globally competitive cyber security sector that enhances Australia's future economic growth

As part of this mission, AustCyber aims to be an independent national body that improves the alignment of disparate cyber security initiatives and investments across industry, the research community, academia and government.

AustCyber is part of the Australian Government's A$250 million Industry Growth Centres Initiative, which aims to tap new sources of economic growth by maximising the country's competitive advantage in six knowledge-driven, high-value sectors.

AustCyber has been leading significant efforts to accelerate and sustain Australia's cyber security sector, including vital activities to counter the challenges highlighted in Chapter 3.

AustCyber is contributing to the sector's strategic goals for growth by 2023 by promoting research, innovation and commercialisation; establishing robust export pathways for Australian capabilities; and implementing a national platform for skills development and workforce growth.

AustCyber's support for the cyber security sector includes:

- undertaking 28 industry-led research and commercialisation projects funded through the $15 million AustCyber Projects Fund, contributing close to $35 million to the economy;
- establishing a National Network of Nodes across states and territories;
- providing startups with resources and connections;
- promoting Australian cyber security providers through missions to the US, UK, Israel, Singapore and Indonesia;
- nationally coordinating the development of a standard TAFE cyber security curriculum that has been introduced across Australia;
- introducing education programs that target schools, higher education institutions, accelerators and business directors;
- partnering with industry and government to identify, lead and implement policy changes that strengthen the regulatory framework for the sector;
- hosting Australian Cyber Week annually to showcase the ecosystem; and
- establishing the National Missing Persons Hackathon in collaboration with the Australian Federal Police and TraceLabs (Canada).

Industry-led collaborations under AustCyber's Projects Fund delivered significant impact towards education, research and the commercialisation of cyber security

Aim and scope

To help the Australian cyber security industry grow and take ideas global.

Projects must be:

- industry-led
- supported by matched funding

Total funding: **$15 million**

Length of initiative: **three years**

Round 1

10 projects funded $6.5 million

Ten projects

Round 2

18 projects funded $8.5 million

18 projects

Assessment criteria

1. Technology Readiness
2. Alignment with knowledge priorities
3. National benefit

$15M = $6.5M + $8.5M >

$100+ million in direct and indirect impact to the economy

Examples of projects funded

Fund Recipient	Forticode	CYBERMERC	THE UNIVERSITY OF SYDNEY
Funding amount	**Industry funding:** $1,285,450 **AustCyber funding:** $1,285,450	**Industry funding:** $1,220,000 **AustCyber funding:** $1,220,000	**Industry funding:** $618,464 **AustCyber funding:** $611,971
Type	Product development	Product development	Education
Description	Forticode was awarded a project to the value of $2,570,900 to leverage their Cipherise™ trusted identify platform which provides technology to support singular, personally-held digital identities, stored and managed on mobile devices. The project will create a highly scalable cryptographic based technology that can interface with both the physical and virtual worlds; allow for independent authentication of personal data and bi-directional communication to confirm intent, and; utilises quantum tolerant technologies and techniques.	Cybermerc have been awarded a project to the value of $2,440,000 to establish a national threat sharing portal, AUSHIELD DEFEND, to collect and share data of new cyber attacks targeting Australian businesses. Enterprise and research partners can now use AUSHIELD DEFEND to test and develop next generation defensive cyber strategies.	The University of Sydney was awarded a project to the value of $1,230,435 to deliver, with Australia and New Zealand Banking Group Limited (ANZ), Commonwealth Bank of Australia (CBA), National Australia Bank Limited (NAB), Westpac Banking Corporation and British Telecom, cyber security challenges for high school students that develop cyber security skills and attitudes, and increase careers awareness.

CASE STUDY

Funding the future of digital identity management

AustCyber's Projects Fund grant recipient truuth has been developing a digital identity platform for user identity verification, while protecting user privacy.

truuth uses technology that fragments, salts (injects false information), encrypts and shards user credentials across multiple trusted servers. The platform delivers a wide range of micro-services that improve online safety and eliminate the need to remember many different passwords, whilst ensuring no single entity has access to a user's biometric data. The truuth platform is being deployed for enterprise customers including Macquarie Bank, NuMobile and Australian Finance Group (AFG).

"Most venture capital funds are focused on scale-ups that already have enterprise customers, while private equity is typically looking to invest A$5-10 million in Series A rounds," said Mike Simpson, CEO & Co-founder of truuth. "AustCyber complements these by supporting early stage companies with highly innovative technology solutions."

The truuth suite of digital identity and authentication services addresses deficiencies of current solutions such as reliance on insecure passwords. It also provides enterprises with higher levels of user authentication by using Artificial Intelligence (AI) and Machine Learning (ML) models to verify the user is present during the authentication event.

AustCyber funding support has been integral to the success of truuth.

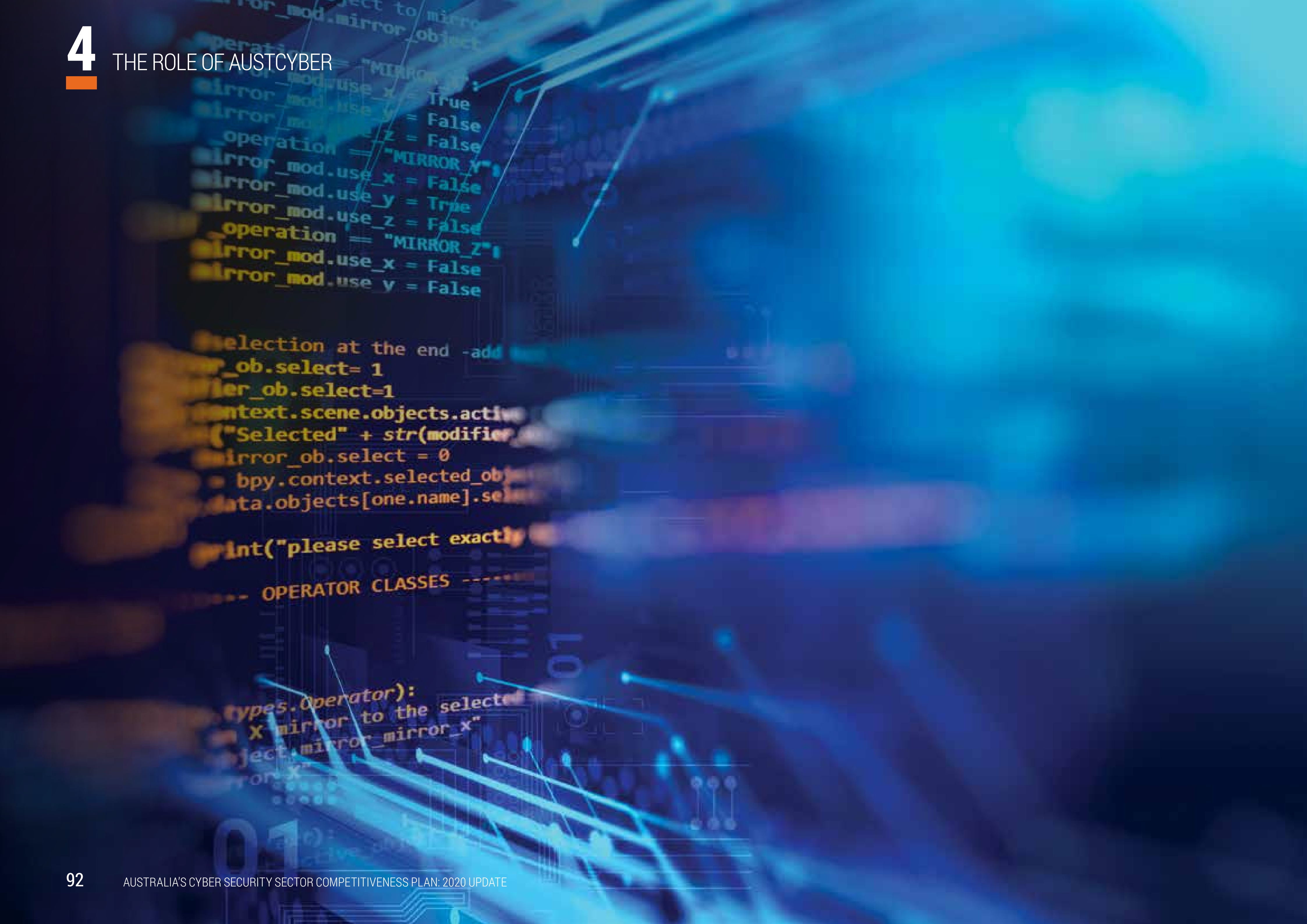
"The Projects Fund enabled us to match funding from private investors to grow the team more rapidly and deliver our digital identity services far earlier," said Mr Simpson. "truuth's successes over the past 12 months would not have been possible without the assistance of AustCyber. Our participation in AustCyber forums has also opened up commercial conversations in the public and private sectors."

truuth

The company provides a range of digital identity services including truuth KYC (Know-Your-Customer), truuth liveness, truuth faceKey and truuth biopass. These services help to safeguard against the recent and rapid rise in 'deep fake' identities created by artificial intelligence and machine learning algorithms which are exacerbating fraud risks.

Recent estimates by the Attorney-General's Department indicate that identity crime costs Australia upwards of $1.6 billion each year, with the majority lost by individuals through credit card fraud, identity theft and scams.[1]

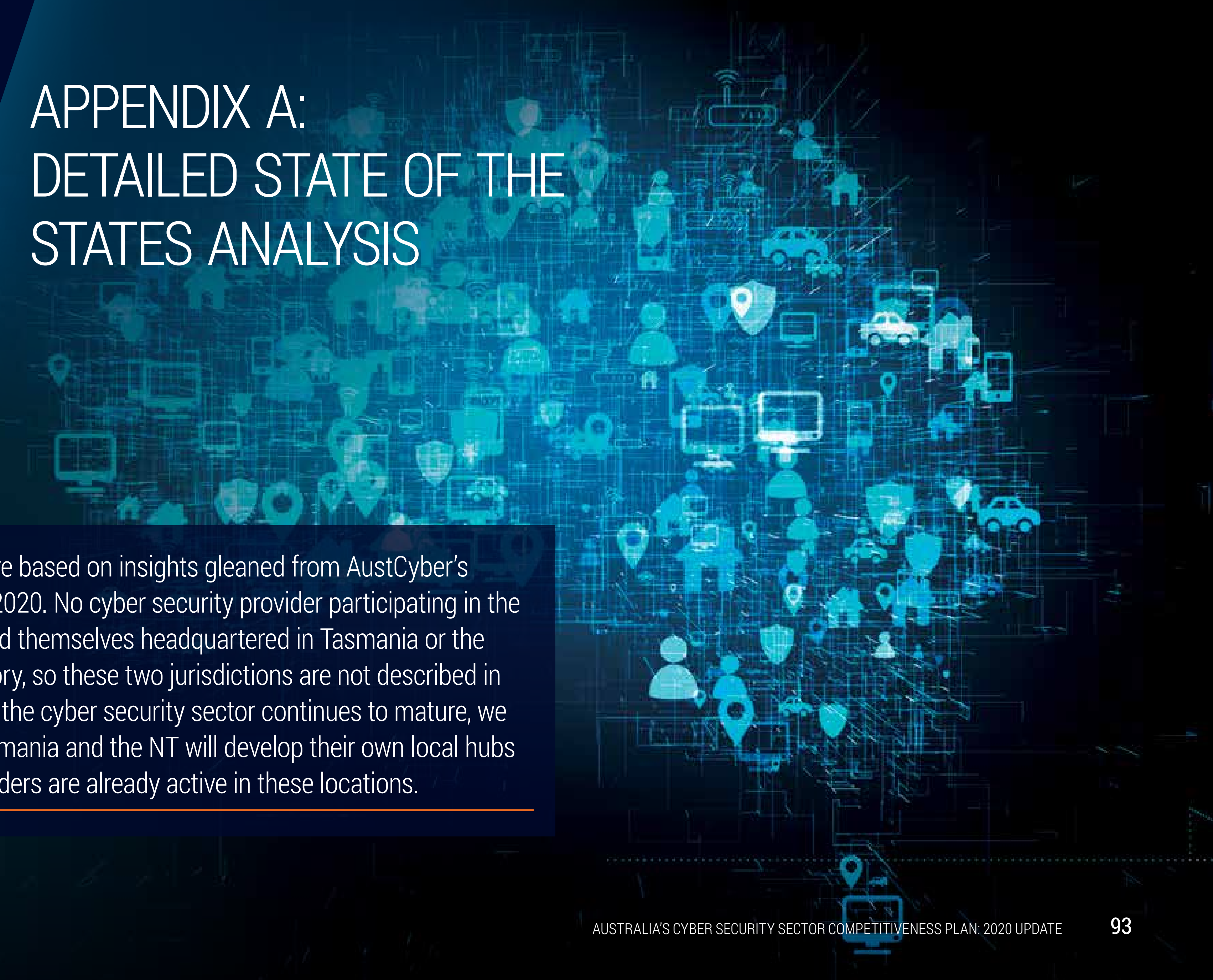
[1] AustCyber (2020), *trUUth: A next generation solution for digital identity and cyber security.* Available at: https://www.austcyber.com/news-events/truuth-next-generation-solution-digital-identity-and-cybersecurity



A

APPENDIX A: DETAILED STATE OF THE STATES ANALYSIS

State profiles are based on insights gleaned from AustCyber's Digital Census 2020. No cyber security provider participating in the Census recorded themselves headquartered in Tasmania or the Northern Territory, so these two jurisdictions are not described in this section. As the cyber security sector continues to mature, we expect that Tasmania and the NT will develop their own local hubs as several providers are already active in these locations.



The ACT has a strong community of cyber security providers that are focused on servicing government and defence clients

Overview

Relative to population, there are more cyber security workers in the ACT than in any other state or territory in Australia.[1] The ACT hosts an active startup community, the members of which have formed collaborative relationships with each other to meet the needs of large clients, including Australian Government agencies.

Provider snapshot

The average age of ACT cyber providers is 7.5 years, slightly below the national average of 8.5 years, and 44 per cent of the ACT's providers were founded less than five years ago. Providers such as WorldStack, Cybermerc, Quintessence Labs, Penten, and FifthDomain are examples of the ACT's vibrant startup community, which is supported by the Canberra Innovation Network, as well as universities including the Australian National University (ANU) and the University of New South Wales (UNSW).

The top three products and services offered by ACT cyber providers are cyber governance and risk, penetration testing, and threat intelligence analytics. The ACT is a training hub for cyber security, and a centre of research and development that spans universities, Australia's national security agencies and the startup community.

At 29 per cent, well below the national average of 43 per cent, the ACT has the lowest rate of cyber providers exporting of any of the states or territories. This is in part due to ACT providers' specialty in serving Australian Government agencies, which can often make it difficult to serve equivalent clients overseas, especially if selling to defence or national security.

Education, skills and research

The ACT is a major centre of cyber security education and research, hosting several important institutions including the Australian Centre for Cyber Security at UNSW Canberra, and the College of Engineering and Computer Science and National Security College at the ANU. The ACT is also home to AustCyber's national office and the Canberra Cyber Network – a partnership between ANU, UNSW Canberra, Data61, University of Canberra and Canberra Institute of Technology.

Territory government support

The ACT Government has identified cyber security as a driver of job creation in Canberra and the Territory's digital strategy recognises the important role that cyber security plays in helping build the 'government of the future'. This commitment to innovation is exemplified by the government's $607,000 funding boost to the Canberra Innovation Network, which aims to connect innovation and entrepreneurship with the territory's strong capabilities in science and research.

[1] Calculated using population and number of cyber security employees

Australian Capital Territory cyber security sector

Overview

Average provider age: 7.5 years

44 per cent of providers are less than five years old

29 per cent of providers are exporting

Cyber priority areas:

1. Tertiary and research sector
2. Defence industry
3. Renewable energy
4. Federal government

~1,700 estimated cyber security workers

Cyber educational institutions

Australian National University

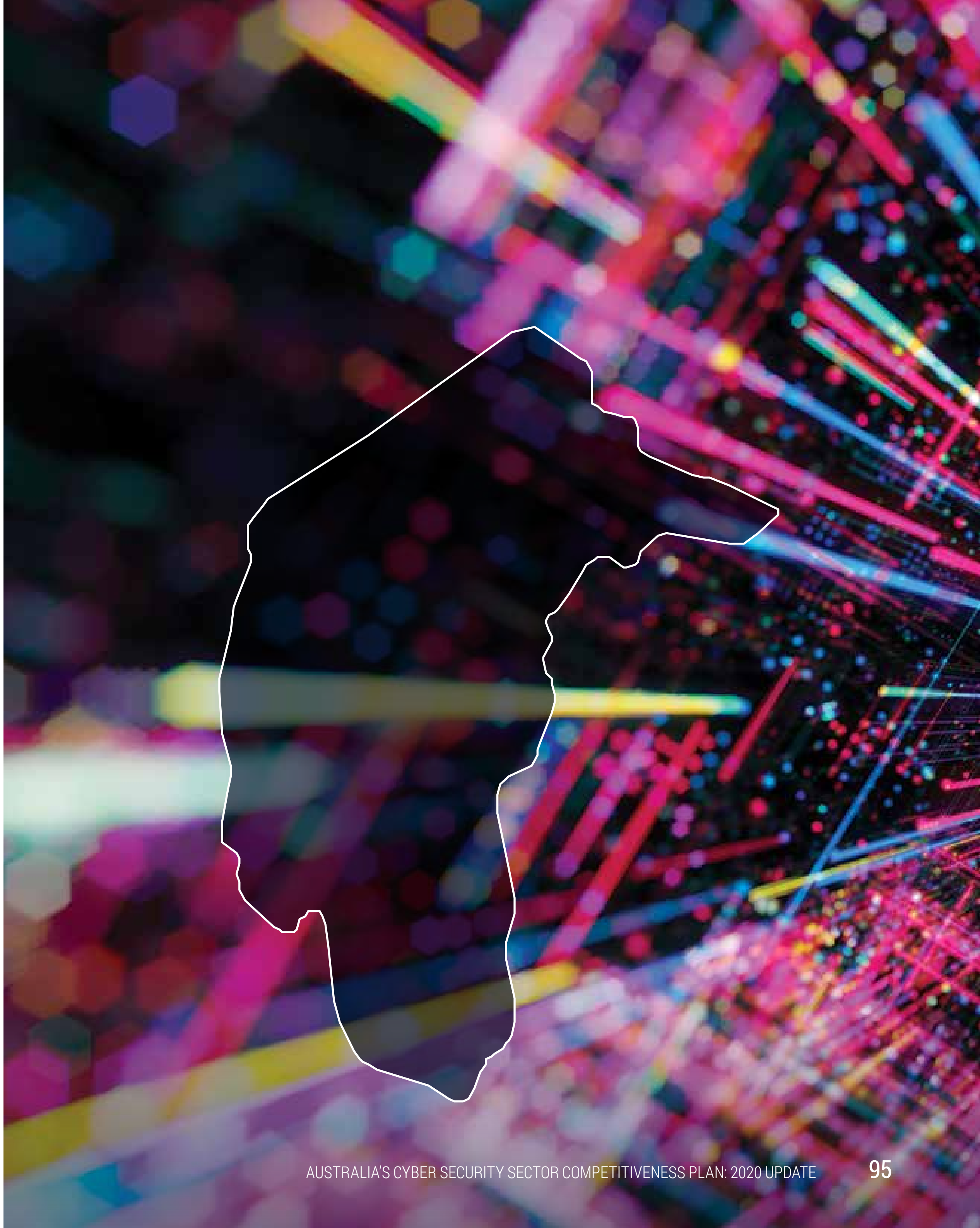
UNSW CANBERRA

Canberra Institute of Technology

UNIVERSITY OF CANBERRA

ACU AUSTRALIAN CATHOLIC UNIVERSITY

Sources: AustCyber's Digital Census 2020, AlphaBeta analysis



New South Wales hosts the largest and most diverse range of cyber security providers in Australia

Overview

More than 80 cyber security providers are headquartered in NSW, 75 per cent of which service the financial services sector. Cyber security providers in NSW are also extending their involvement to bourgeoning technologies, such as advanced manufacturing and automation (Industry 4.0).

Provider snapshot

The average age of cyber security providers in NSW is 8.5 years.

NSW has a growing cyber startup community, with notable success stories such as Secure Code Warrior, Huntsman Security and Kasada, and a plethora of new entrants such as Paraflare, Daltrey and Tikabu. The NSW Government has helped startups scale by establishing the Cyber Security Connect Program, which aims to build networking and collaboration opportunities between the sector and the wider NSW economy. The government has also launched a Cyber Security Vulnerability Management Centre in Bathurst to monitor its online assets, in partnership with Australian born UpGuard.

Providing cyber governance and risk services is the state's top cyber offering by revenue. These services are in high demand among professional and financial services providers, many of which are based in Sydney. The NSW Government is also beginning to invest strongly in digital technology, rolling out several significant projects – such as the Future Transport Strategy, Smart Places Strategy and Digital Restart Fund – to drive demand for cyber.

Only 38 per cent of NSW's cyber security providers are exporting – below the national average of 43 per cent – and more than one-third of those surveyed cited gaining access to export markets as a key barrier to growth.[1] There are notable exceptions: companies such as Secure Code Warrior have had significant success helping overseas clients improve the security of their coding practices.

Education, skills and research

Several of NSW's major universities offer cyber security at both graduate and post-graduate levels. For example, Macquarie University offers a Bachelor of Cyber Security and UNSW, through its cyber centre of excellence, offers a Master of Cyber Security and works closely with the Defence Research Institute.

TAFE NSW offers the Certificate IV in Cyber Security. TAFE NSW partnered with the NSW Cyber Security Innovation Node this year, supported by Hewlett Packard, to launch cyber security mini-modules online to help workers retrain as the COVID-19 pandemic drives more businesses to digitise and rely on online tools.

The cyber security research landscape continues to build in NSW, led by UNSW's CySPri Laboratory which conducts cyber security research on topics such as application and network security, and collaborates with several industry partners.

State government support

The NSW Government recently announced a $1.6 billion Digital Restart Fund, to further drive digitisation of services across government agencies. Of this total amount, $240 million has already been committed to enhancing the government's own cyber security, to be articulated in the NSW Cyber Security Strategy.

[1] AustCyber's Digital Census 2020

New South Wales cyber security sector

Overview

Average provider age: 8.5 years

40 per cent of providers are less than five years old

38 per cent of providers are exporting

Cyber priority areas:

1. Industry 4.0
2. Cross sectoral digital transformation
3. Cyber workforce development
4. Financial services

~10,150 estimated cyber security workers

Cyber educational institutions

Charles Sturt University Australia

Macquarie University Sydney · Australia

Western Sydney University

University of Wollongong Australia

UNSW Australia

UTS University of Technology Sydney

NSW Government | TAFE NSW

The University of Newcastle Australia

Sources: AustCyber's Digital Census 2020, AlphaBeta analysis

Queensland's cyber security providers are stong exporters, with nearly 60 per cent reporting overseas customers

Overview

Queensland's cyber security sector has relative strengths in servicing the government sector: more than 75 per cent of survey respondents identified federal or state government as a key customer. Compared to other states, Queensland providers have a high export rate: nearly 60 per cent are selling cyber security products or services overseas. In mid-2020, AustCyber announced that it would be opening three Cyber Security Innovation Nodes in Brisbane, Townsville and the Sunshine Coast, which will further build on the state's cyber capability and assist to protect national critical infrastructure.

Provider snapshot

Queensland is home to relatively mature cyber providers, with an average age of ten years – second only to South Australia. Although Queensland has a relatively small startup community, with only 32 per cent of providers less than five years old, it is home to exciting startups including Assetnote, SecureStack and CyberMetrix. Cyber providers of all ages can find support in the Queensland Government's Advance Queensland Strategy, a suite of programs and grants designed to drive the knowledge and jobs of the future.

The top cyber products and services offered in Queensland are penetration testing, cyber governance and risk services, and application security. The state government's recent focus on growing Queensland's innovation ecosystem through its Advance Queensland Strategy will likely shape the state's future cyber product mix, as providers respond to key priority areas such as robotics and agricultural technology (agritech).

Export appears to be a strength for Queensland cyber providers, with nearly 60 per cent exporting their products and services overseas. One prominent success story is ASX-listed RightCrowd, which has had significant success internationally with its identity access management and threat intelligence analytics solutions.

Education, skills and research

Queensland's educational institutions are stepping up to address the cyber security skills shortage with a range of graduate and postgraduate cyber courses now on offer. This is led by the University of Queensland (UQ) who recently launched their interdisciplinary Master of Cyber Security program. The Queensland University of Technology, Griffith University, University of the Sunshine Coast and the University of Southern Queensland all offer postgraduate level cyber security courses. UQ also has a cyber security research centre which explores emerging cyber areas such as IoT and cyber physical security and secure communications for space.

State government support

The Queensland Government has awarded a $250,000 grant to the Australian Information Industry Association to partner with Queensland University of Technology to deliver critical skills around innovation in cyber security. Queensland was also the first state to launch a Joint Cyber Security Centre within the Australian Cyber Security Centre.

Overview

Average provider age: ten years

32 per cent of providers are less than five years old

58 per cent of providers are exporting

Cyber priority areas:

1. Defence
2. Advanced manufacturing
3 Health
4. Education
5. Agritech
6. Federal and state government

~3,600 estimated cyber security workers

Cyber educational institutions

Griffith University

The University of Queensland Australia

QUT

University of Southern Queensland

USC Australia

tafe Queensland

Sources: AustCyber's Digital Census 2020, AlphaBeta analysis

South Australia's cyber providers have an exciting opportunity to collaborate with Australia's emerging industries

Overview

The development of South Australia's innovation precinct, Lot Fourteen, presents an exciting opportunity for cyber providers to collaborate with emerging areas such as machine learning and the space industry. This will add to the state's expertise in servicing the defence sector and further build on its export strengths.

Provider snapshot

Although South Australia has a relatively small pool of fully dedicated cyber security providers, it is home to Australia's most mature providers at an average age of 11 years – well above the national average of 8.5 years. Although cyber is just one part of their businesses, South Australia is home to well-established providers such as Prophecy International and Consunet, which have been operating for 28 and 18 years respectively. The state also has a small number of promising young providers, such as Airlock Digital and CyberOps.

The high value of defence contracts in South Australia has spurred the development of products and services tailored to the defence industry, such as penetration testing. The positive impacts of Lot Fourteen are also beginning to surface, with CyberOps offering solutions tailored to the space and IoT sectors.

The maturity and quality of South Australia's cyber security providers is reflected in the fact that it's the leading state for cyber exports, with 67 per cent of its providers selling overseas. One example of overseas success is Airlock Digital, which has a global reputation for its application whitelisting solution.

Education, skills and research

South Australia hosts five important education institutions. The University of Adelaide, Flinders University, University of South Australia and Torrens University offer degrees in cyber security at both undergraduate and postgraduate level; whilst TAFE South Australia offers the Certificate IV in Cyber Security. The University of Adelaide also runs an online cyber security course for teachers, providing a critical resource to improve cyber education in schools.

In 2020, the South Australian Government established the Australian Cyber Collaboration Centre at Lot Fourteen which aims to support Australian cyber providers to launch new products and services globally. Flinders University has also launched the Jeff Bleich Centre for the US Alliance in Digital Technology, Security and Governance which focuses on research into issues such as foreign interference in democratic elections and national security.

State government support

The Government of South Australia has a clear strategic plan for cyber security that is centred around innovation and collaboration with industry, supported by the Australian Cyber Collaboration Centre and Lot Fourteen.

South Australian cyber security sector

Overview

Average provider age: 11 years

33 per cent of providers are less than five years old

67 per cent of providers are exporting

Cyber priority areas:

1. Defence industry and supply chain
2. Autonomous systems
3. Space industry
4. Digital health

~1,000 estimated cyber security workers

Cyber educational institutions

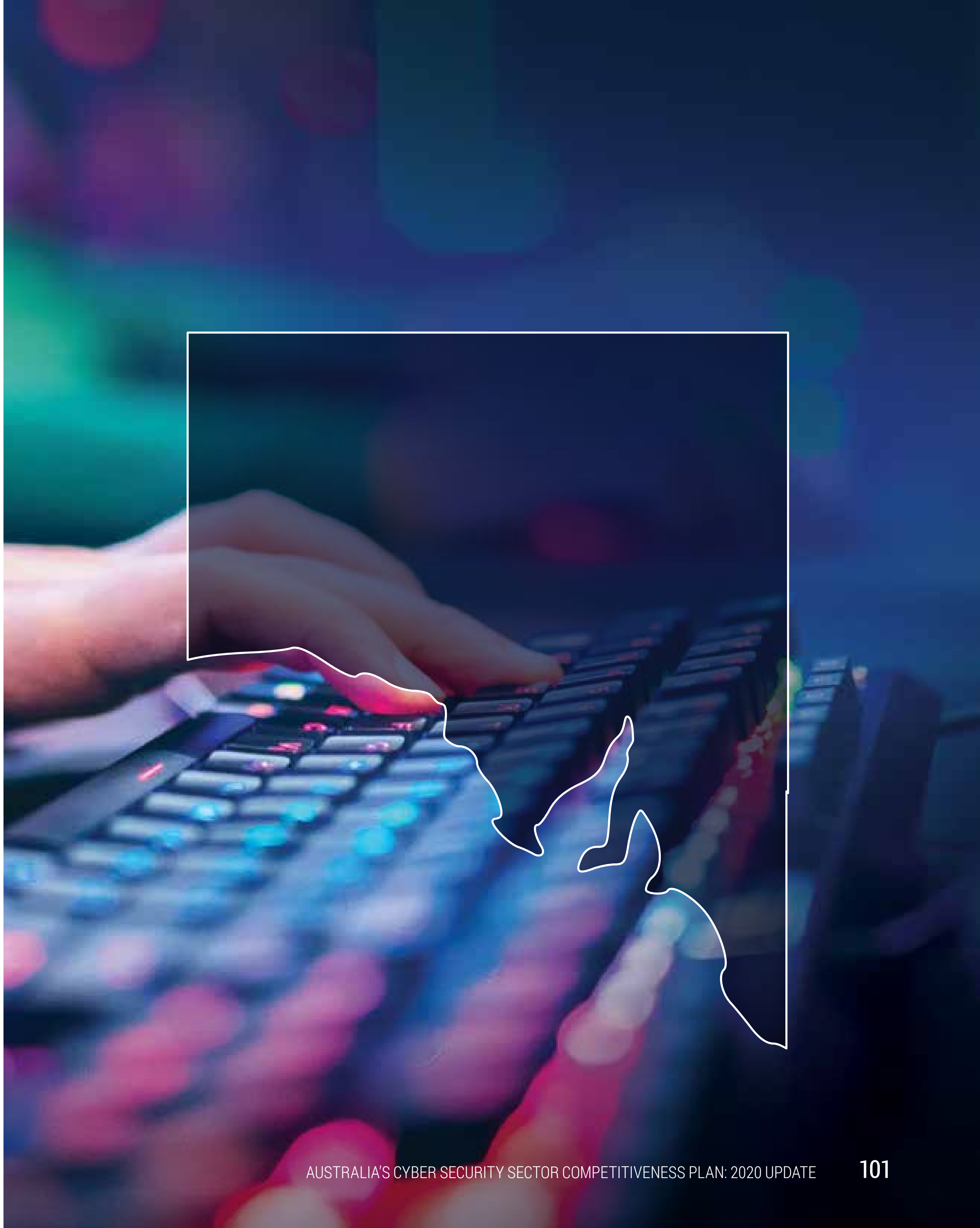
University of South Australia

THE UNIVERSITY of ADELAIDE

Flinders UNIVERSITY

tafeSA

Sources: AustCyber's Digital Census 2020, AlphaBeta analysis



Victorian cyber security providers have strengths in servicing the financial and defence sectors, and significant success abroad

Overview

Victoria has the second largest cyber security workforce in Australia, with nearly 9,000 workers. As in NSW, financial services is the most prominent customer segment for Victorian providers: over 75 per cent of surveyed cyber security firms active in Victoria are servicing this sector. Defence is also a large customer of Victorian cyber providers: approximately 57 per cent of Victorian providers service defence organisations.

Provider snapshot

At an average age of 7.5 years, Victoria's cyber providers are just slightly younger than the national average of 8.5 years. 42 per cent of Victorian cyber providers were founded less than five years ago, including notable new providers such as VeroGaurd, HackHunter, Retrospect Labs and Cynch Security. There is a strong support network for young providers in Victoria, including from government programs such as LaunchVic, and the state hosts Australia's only cyber security accelerator, CyRise. As well as having its share of startups, Victoria has produced some of the nation's most successful cyber providers, such as ASX-listed Tesserent and newly established CyberCX.

Consistent with Victoria's large population and diversity of businesses, the state's cyber providers offer a breadth of cyber products and services. The top three cyber products offered in Victoria are cyber governance and risk services, penetration testing, and mobile and web security.

As a promising sign that Victorian cyber providers are able to compete globally, 46 per cent of Victoria's cyber providers are exporting, which is above the national average of 43 per cent. One example of this is MailGuard, an email security provider that has a global customer base.

Education, skills and research

Victoria is home to a rich network of cyber research and education institutions including RMIT, Deakin University and the University of Melbourne, which hosts an Academic Centre of Cyber Security Excellence. The Oceania Cyber Security Centre is also based in Melbourne, which is a cooperative organisation made up of eight Victorian universities and CSIRO's Data61. Further adding to the state's cyber research capability is the Defence Science Institute which is a collaboration between the University of Melbourne, Victoria's state government, and the Australian Government's Defence Science and Technology (DST) Group.

State government support

The Victorian Government Cyber Security Strategy 2016-2020 outlines the measures being taken to ensure cyber reliance and governance in the public and private sectors. As part of this strategy, the government has committed $17.6 million to further develop its cyber capabilities.

Victoria cyber security sector

Overview

Average provider age: 7.5 years

42 per cent of providers are less than five years old

46 per cent of providers are exporting

Cyber priority areas:

1. Digital health
2. Skills and education
3. Financial services
4. Defence

~8,300 estimated cyber security workers

Cyber educational institutions

MONASH University
RMIT UNIVERSITY
DEAKIN UNIVERSITY AUSTRALIA
SWINBURNE UNIVERSITY OF TECHNOLOGY
VICTORIA UNIVERSITY
holmesglen
LA TROBE UNIVERSITY
BOX HILL INSTITUTE
THE UNIVERSITY OF MELBOURNE
Federation UNIVERSITY · AUSTRALIA
Chisholm
MELBOURNE POLYTECHNIC

Sources: AustCyber's Digital Census 2020, AlphaBeta analysis

Western Australia is home to the youngest cyber security providers, about half of which were founded less than five years ago

Overview

The average age of cyber security providers in Western Australia is seven years. Given the state's abundant natural resources, cyber security providers specialise in servicing large mining, oil and gas companies. Western Australia's educational institutions offer some of the most expansive and high-quality cyber security qualifications in the country.

Provider snapshot

Approximately half of all cyber security providers in Western Australia were founded less than five years ago, which demonstrates the emerging nature of the state's cyber sector. Some of the most promising startups coming out of Western Australia include Sapien Cyber, which has developed a threat detection and vulnerability management solution, and Red Pirahna, who provide a unified threat management platform. Western Australia's startup and the Australian Government's Entrepreneurs' Programme play a critical role in supporting Queensland's startup sector.

The top products and services for Western Australian cyber providers are cyber governance and risk services, penetration testing, and cyber security delivery such as managed security services and security operation centres. An emerging provider of cyber security services is CSO Group, which specialises in cyber security risk consulting.

The relative youth of Western Australia's cyber providers is evidenced in the fact that only one-third have customers overseas – they are focusing on building their strengths locally. Once these providers are globally competitive, their unique location will make Asian markets more accessible than for their eastern counterparts, which will increase export opportunities.

Education, skills and research

Pioneered by Edith Cowan University (ECU), Western Australia has long been a leader in cyber security education. ECU has the widest range of both graduate and postgraduate cyber security courses in Australia and consistently record some of the strongest enrolment numbers in cyber security across the country. ECU has been recognised by the Australian Government as an Academic Centre of Cyber Security Excellence and is home to the Security Research Institute which focuses on cyber systems, critical infrastructure security and cybercrime. The Cyber Security Cooperative Research Centre is also based in Western Australia.

State government support

The Government of Western Australia has allocated a $16.7 million New Industries Fund. In response to COVID-19, the fund committed $800,000 to allow SMEs to address cyber security attacks as a result of having to move their operations online. In 2018, the state government announced a partnership with ECU to ensure the increased security of Western Australia's public sector.

Western Australia cyber security sector

Overview

Average provider age: seven years

50 per cent of providers are less than five years old

33 per cent of providers are exporting

Cyber priority areas:

1. Mining
2. Oil and gas services
3 Agritech
4 Operational Technologies (OT)

~1,400 estimated cyber security workers

Cyber educational institutions

TAFE International Western Australia

Curtin University

Australia ECU Edith Cowan University

Murdoch University Perth | Singapore | Dubai

Sources: AustCyber's Digital Census 2020, AlphaBeta analysis

B

APPENDIX B: CYBER TAXONOMY

Cyber security product categories

As digital technology evolves, so does cyber security. To the layperson, cyber security might mean firewalls and off-the-shelf anti-virus software, but that limited scope is no longer accurate. Protecting digital assets is now multidisciplinary, and cyber security today involves anything from tools and technologies to behavioural practices and procedures.

Cyber security has traditionally been understood in terms of hardware, software and services. The diversity and sophistication of modern cyber security means that this categorisation is no longer appropriate.

The Cyber Security Body of Knowledge (CyBOK) is a international collaboration headed by the University of Bristol that structures cyber security according to five main categories:

- **Infrastructure security:** securing computer and digital networks and related physical hardware and systems from intruders and intrusions, whether targeted or opportunistic.
- **Systems security:** operational, network and systems security that includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- **Software and platform security:** security that focuses on keeping software and an entire computing platform and devices – including mobile, cloud and web applications – resilient to cyber threats. This includes information security that protects the integrity and privacy of data, both in transit and at rest.
- **Attacks and defences:** a proactive and adversarial 'attack' approach to protecting against cyber attacks, which includes penetration and vulnerability testing as well as ethical hacking. Defensive security focuses on reactive measures such as patching software and detection.
- **Human, organisational and regulatory aspects:** tools and services to protect against intentional and unintentional user mistakes; support observance of organisational governance and policies; and enforce compliance with regulatory requirements.

This new framework provides a more robust foundation for researchers, policymakers and industry to study the sector.

Cyber security product categories

Segment of the cyber sector	Examples
Infrastructure security	• Managed security service provider • Security operations centres • Security hardware and physical systems
System security	• Cryptography • Operating systems, network, cloud, quantum control and autonomous systems security • Authentication including biometrics • Identity access management
Software and platform security	• IoT security • Software as a service (SaaS) • Threat intelligence analytics • Mobile, web and application security
Attacks and defences	• Penetration testing • Bug bounty programs • Threat detection and response • Wargaming and exercising • Cyber deception technologies • Digital forensics
Human, organisational and regulatory aspects	• Governance, risk and compliance management • Readiness and maturity audits • Privacy impact assessment • Training and education • Cyber-related professional services

Research methodology

Output	Description	Approach	Data sources
Cyber security spending	• Business and consumer spending on cyber security products and services in Australia.	• Spending on cyber security in Australia was estimated using the weighted average of external market research estimates, as well as previous SCP modelling.	• Gartner[1] • IBISWorld[2] • 2019 SCP measurement model
Sector revenue	• The amount of revenue that accrues to cyber security providers where their core activities take place in Australia (includes both Australian- and foreign-owned providers).	• A proprietary model was developed to estimate the proportion of total spend that is captured in Australia (as opposed to being imported), as well as the amount of export revenue captured by cyber providers in Australia. • Expert interviews with leading representatives from industry, government and academia informed the key assumptions in the model, such as the market share of providers with core business in Australia, and the proportion of revenues derived from exports. • To further validate the sector measurement model in a bottom-up way, analysis on aggregated revenue data from the Digital Census was performed, supplemented with illion revenue data to fill in gaps for providers that did not respond to the survey.	• Gartner[1] • IBISWorld[2] • Expert interviews • AustCyber's Digital Census 2020 • Illion[3]
Employment	• Employees in the cyber security sector, as well as those in internal cyber security roles such as chief information security officers and in-house cyber teams.	• ABS data on total output and employment figures was used to estimate the revenue generated per job for cyber-related roles. • Sector revenue estimates were then used to estimate the number of jobs in the cyber sector. • Informed by expert interviews, an assumption of the rate of internal cyber security spending per dollar of external cyber spending was applied to estimate the number of jobs in internal cyber security roles.	• Gartner[1] • IBISWorld[2] • Expert interviews • Australian Bureau of Statistics (ABS)
Gross value added (GVA)	• Measuring the cyber security sector's GVA reveals its direct contribution to the size of Australia's economy.	• GVA is made up of profit and returns to workers (wages). • Sector profit was estimated using the weighted average profit margin of over 100 survey respondents. This was applied to top-down revenue estimates (factoring in depreciation, amortisation and tax). • A weighted average wage-to-revenue ratio for the sector was determined using survey responses. This was applied to top-down revenue estimates to estimate total wages for the sector.	• Gartner[1] • IBISWorld[2] • AustCyber's Digital Census 2020 • illion[3]

1. Gartner (2020), *Forecast: Information Security and Risk Management, Worldwide, 2018–2024, 2Q20 Update*. Available at: https://www.gartner.com/en/documents/3988093/forecast-information-security-and-risk-management-worldw
2. IBISWorld (2020), *IT Security Consulting in Australia*. Available at: https://www.ibisworld.com/au/industry/it-security-consulting/4050/#:~:text=Revenue%20in%20the%20IT%20Security,two%20years%2C%20constraining%20industry%20demand and *Data processing and web hosting services in Australia*. Available at: https://www.ibisworld.com/au/industry/data-processing-web-hosting-services/2246/
3. Customised data from illion

AustCyber's mission is to grow a vibrant and globally competitive cyber security sector that enhances Australia's future economic growth.

NODE 01
NODE 04
NODE 05
NODE 02
BLOCK 01
BLOCK 01
NODE 01
NODE 02
operation == "MIRROR_X":
mirror_mod.use_x = True
mirror_mod.use_y = False
mirror_mod.use_z = False
operation == "MIRROR_Y":
mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True
selection at the end -add
ob.select= 1
er_ob.select=1
ntext.scene.objects.activ
"Selected" + str(modifie
irror_ob.select = 0
bpy.context.selected_ob
ata.objects[one.name].se
int("please select exactl
OPERATOR CLASSES ----
types.Operator):
X mirror to the selected
ject.mirror_mirror_x"
mirror X"
context):
object is not

Contact

Email:	info@austcyber.com
Phone:	0455 260 848
Website:	www.austcyber.com
Twitter:	@AustCyber @Cyber_Roo
LinkedIn:	AustCyber – The Australian Cyber Security Growth Network Ltd

Australian Government
Department of Industry, Science, Energy and Resources
Industry Growth Centres

AustCyber
Australian Cyber Security Growth Network