Australia’s Cyber Security Sector Competitiveness Plan 2022

Supporting the development of a vibrant and globally competitive Australian cyber security sector

AustCyber
Part of the Stone & Chalk Group.

At a glance

Designed to help shape, inform and grow Australia's cyber security sector

AustCyber, part of the Stone & Chalk Group, has a clear mission to support the development of a vibrant and globally competitive Australian cyber security sector.

We exist to grow Australia's cyber security ecosystem, export our cyber security to the world, and make Australia the leading centre for cyber-education.

Our 2022 SCP flagship publication highlights the criticality for businesses to protect themselves from cyber threats, and the importance of ensuring our young cyber security sector receives the necessary support to grow and thrive competitively.

2022 highlights

Australia's cyber security sector will contribute an estimated **$2.4 billion** to the country's Gross Domestic Product in 2022, up from **$2.2 billion** in 2020.

Australia's cyber sector annual revenue growth has averaged **8.7 per cent over the past five years** – slower than other leading cyber jurisdictions.

Australia experienced **745 cyber attacks per day** (one every two minutes) in 2021.

The number of cyber attacks in Australia is expected to **double in the next five years**.

47,000 people are employed in cyber security roles in Australia (2022), making it a larger employer than the medical technology sector.

Australian cyber security firms are focused on servicing a relatively small domestic market. The Australian market represents only **2.1 per cent of global cyber security demand**.

Australian cyber security **startups receive 300 times less funding** than international peer leaders.

A cyber attack against Australia (modelled in the 2022 SCP) could **cost up to $12.6 billion**.

2026 outlook

Australia could increase its annual cyber security revenue by **$800 million by 2026**, if it acts on the growth barriers identified in the SCP.

Australia's annual cyber security revenue growth is forecast to be **5.5 per cent by 2026**, almost half of the international leading cyber security jurisdictions **forecast average of 9.9 per cent**.

There will be a shortage of **3,000 cyber security workers** in Australia by 2026.

Future opportunities

To grow revenue, Australia must improve its startup environment, bolster domestic procurement and export capability, and better attract local and international talent.

Improve startup support – Government funding directed to cyber security research has decreased from $9.8 million in 2019 to $7.5 million in 2022.

Continuing to collaborate across sector stakeholders and mature the innovation hubs will support a stronger innovation ecosystem.

Bolster domestic procurement and export capability – The Australian market represents only 2.1 per cent of global cyber security demand. Only 50 per cent of Australian firms are exporting.

Ensuring government procurement processes are accessible to small, local firms will support growth in domestic revenue. Continued trade outreach will facilitate export growth.

Better attract local/international talent – Although there are more people entering the cyber security sector, it is not fast enough to keep up with attrition and increased demand.

Providing incentives and support to train in cyber security will strengthen the talent pipeline. Increasing the number of cyber security skilled migrants will mitigate short-term shortages.

Contents

Executive Summary 2

Acknowledgements 4

Foreword 6

01 **The cyber security sector generates and protects significant economic value for Australia** 8

02 **Australian cyber security sector growth is slower than peers for three reasons** 24

03 **Australia has an opportunity to add $800 million to annual cyber security revenue by 2026 through three key actions** 38

Appendices 44

A.1 State of the sector 44

A.2 AustCyber has made strong progress on its strategic objectives of growing, exporting and educating 68

A.3 Cyber security taxonomy 72

A.4 Value at risk 78

A.5 Methodology 90

Executive Summary

The cyber security sector generates and protects significant economic value for Australia. Ongoing support for the sector is critical.

1 **AustCyber has played an important role in the progression of the Australian cyber security sector.** Driven by the mission of growing, exporting and education since its inception in 2017, AustCyber (now part of the Stone & Chalk Group) has aided the development of a vibrant and growing network of Australian-based cyber security firms. Today, there are an estimated 291 firms in the sector.

2 **The cyber security sector in Australia will contribute an estimated $2.4 billion to the country's Gross Domestic Product** (GDP) in 2022, up from $2.2 billion in 2020. There are 47,000 people working in cyber security roles in 2022, making it a larger employer than the medical technology sector.

3 **Australia's cyber security sector acts as the frontline defence against increasingly frequent and severe cyber attacks**. A cyber attack targeting Australia occurs every two minutes. Experts suggest that this will double by 2027. Recent incidents show how costly and disruptive these attacks can be, with an active network intrusion estimated to cost up to $12.6 billion.

Australia's forecast annual revenue growth of 5.5 per cent is low and slower relative to leading international peers. Australia risks falling further behind unless it addresses three challenges.

1 **Limited startup support** – Australian cyber security startups have limited access to funding and research support. In 2022, Australian startups generated 300 times less funding than Israeli and Canadian startups. Government funding directed to cyber security research has also decreased from $9.8 million in 2019 to $7.5 million in 2022.

2 **Lack of export access** – Australian cyber security firms are focused on servicing a relatively small domestic market. The Australian market represents only 2.1 per cent of global cyber security demand. Australian firms are not yet taking full advantage of the global opportunity, with only 50 per cent of firms exporting and export revenues accounting for a smaller share than other international peers.

3 **Workforce shortages** – There will be 3,000 fewer cyber security workers than required by 2026. There are more people entering the sector, with enrolments and skilled migration numbers growing (albeit at a much slower rate compared to before COVID-19). Yet, this is not fast enough to keep up with attrition from the sector and increased demand.

There is an opportunity for Australia's cyber security sector to catch up with its peers. Australia can add $800 million to its annual cyber security revenue by 2026 through three key actions.

1 **Support research, innovation and startup developmen**t – Increasing R&D funding through ARC grants and increasing the scope and clarity of R&D tax incentives will support cyber security research and industry development. Continuing to collaborate across sector stakeholders and mature the innovation hubs will support a stronger innovation ecosystem.

2 **Bolster domestic procurement and export capability** – Ensuring that government procurement processes are accessible to small, local firms will support continued growth in domestic revenue. Continued trade outreach, including trade delegations, export support and study tours, will facilitate export growth.

3 **Attract local and international talent** – Providing incentives and support for school leavers and skilled workers to train in cyber security will strengthen the cyber talent pipeline. Increasing the number of cyber security skilled migrants will mitigate short-term shortages.

Acknowledgements

AustCyber would like to thank all of the respondents of the Digital Census 2022. The responses captured in the survey have enabled us to present detailed insights into the sector. This 2022 update to Australia's Cyber Security Sector Competitiveness Plan (SCP) was also informed by extensive consultation with governments, the private sector and the research community in Australia and internationally.

AustCyber would like to acknowledge and thank all of those who contributed:

Accenture

Amazon Web Services

Australian Government Department of Industry, Science and Resources

Australian Government Department of Home Affairs

BHP

Insurance Australia Group

(ISC)2

Palo Alto Networks

QBE Insurance Group

Toll Group

Trustwave

The University of Queensland

Westpac

About AustCyber

AustCyber's mission is to support the development of a vibrant and globally competitive Australian cyber security sector. In doing so, we will enhance Australia's future economic growth in a digitally enabled global economy. AustCyber exists to grow Australia's cyber security ecosystem, export our cyber security to the world, and make Australia the leading centre for cyber education.

In 2021, AustCyber joined the Stone & Chalk Group, together focusing on creating the next generation of cyber-secure emerging tech companies, to drive Australia's economy into the next decade and beyond.

AustCyber is part of the Australian Government's 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. And continues to contribute 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.

Visit **www.austcyber.com** to sign up to be a 'Friend of the Network' and receive the latest updates on AustCyber's events and activities.

Foreword

This year's Sector Competitiveness Plan (SCP) has been developed with over 60 Australian Cyber Security companies and experts. As AustCyber's flagship publication, it is designed to help shape, inform and grow Australia's vibrant and globally competitive cyber security sector.

As the CEO of the Stone & Chalk Group, I am thrilled to launch the first SCP since the merger of AustCyber with the Stone & Chalk Group. We remain committed to continuing our ongoing support of the cyber security needs of all, including startups, scaleups, corporations and government, through our cyber security innovation hubs and nodes across the country.

In the most pressing time of our cyber security history, with cyber security becoming an increasing national concern, it is a critical and opportune time to share knowledge and insights that identify risks and opportunities, drive robust innovative discussion, deliver proposed solutions and encourage healthy national debate on our cyber security industry.

The height of the COVID pandemic over the last few years has required many businesses to accelerate their digital transformation projects, in order to remain open and competitive virtually in physically constrained conditions. This increased digitalisation has helped businesses realise productivity and efficiency benefits much sooner, and we have seen businesses adjust their practices and adopt new hybrid working environments. This has ultimately presented new and emerging cyber security risks, highlighting that it's become more critical than ever before that we all remain vigilant and take responsibility for ensuring good cyber security behaviour.

The more recent Ukraine-Russia conflict has demonstrated that cyber offences and defences are now a critical facet of modern warfare. Increasing cyber security threats are being driven by our rapidly evolving threat landscape, geopolitical tensions, and economic, environmental and supply chain challenges, along with increased regulations such as the critical infrastructure security and foreign investment reforms.

Back home, Australia continues to face a growing cyber security skills shortage across the economy, facing competition for talent between our public and private sectors both locally and globally. In order for our cyber security sector to grow and become sustainable, we must access a sustainable pipeline of talent and skills to meet the future demands of cyber security and emerging high-tech industries. The Federal Government's 12-month consultation, following the Jobs and Skills Summit in September 2022, represents an important opportunity to continue the skills shortage discussion.

This year we returned to the RSA Conference in San Francisco, where we had the pleasure of witnessing Australian cyber security businesses building closer relationships in the US. We're also experiencing increasing trade opportunities that are not just limited to the US, with more governments and businesses around the globe wanting to work with Australia. This gives us great hope and optimism about the future and the opportunity to work closer with our international allies, to continue to support a thriving global cyber security community.

Australia's continuously evolving and complex cyber security environment represents significant challenges as well as opportunities now and well into the future. As such, we strongly welcome the Federal Government's timely announcement to review Australia's Cyber Security Strategy 2020. We believe this review is very much needed to ensure the continual growth of the cyber security sector in Australia.

Stronger cyber security is fundamental to the future of our digitally enabled economy. We continue to witness regular cyber security threats that impact both small and large businesses across a range of industries, as well as our wider community. Our mission at the Stone & Chalk Group is to transform Australia into a sustainable tech-driven economy, and to help achieve this, we play a key role in encouraging businesses at the leading edge of emerging and critical high-tech innovations (including startups and scaleups), to protect themselves from cyber security threats, ensuring our young cyber security sector receives the necessary support to enable it to grow competitively.

This year's 2022 SCP provides key findings around three critical themes related to growth, exports and education for cyber security in Australia. These are fundamental to the sustainability of the cyber security industry in Australia. I commend this SCP and look forward to working with all relevant governments, industry and other key stakeholders in our community to continue to grow Australia's vibrant and globally competitive cyber security sector.

Michael Bromley
CEO Stone & Chalk Group and AustCyber

01 The cyber security sector generates and protects significant economic value for Australia

AustCyber has supported the cyber security sector, which creates benefits for the economy in two ways

AustCyber has played an important role in supporting the cyber security sector to create these benefits

1

The cyber security sector directly contributes to GDP by generating $2.4 billion in Gross Value Added and supporting the employment of 47,000 workers

2

The Australian cyber security sector provides services which protect broader economic activity by deterring cyber attacks and preventing them from causing damage, or reducing the associated damage

AustCyber plays an important role in protecting Australia against cyber attacks, by supporting the Australian cyber security sector in three areas

1 Grow

Grow an Australian cyber security ecosystem

AustCyber aims to grow the Australian cyber security ecosystem by providing funding, information and programs to support organisations in the sector.

Some examples include:

- **The Projects Fund**
  A $15 million initiative helping Australian cyber security firms to grow and take their ideas global. 27 small and medium-sized enterprises (SMEs) have received funding from the Projects Fund over three years.
- **AUCYBERSCAPE**
  AustCyber created AUCYBERSCAPE as Australia's first national cyber security digital ecosystem, showcasing Australian cyber security capability and opportunities globally. Currently, 291 Australian cyber security firms are registered with AUCYBERSCAPE making it easy for Australian businesses to find a cyber security firm that suits their needs.
- **AUCyberExplorer**
  AustCyber created AUCyberExplorer, an interactive map that provides detailed and actionable supply and demand data on the cyber security workforce, jobs and career pathways.
- **GovPitch 2020**
  This program selected 11 businesses from a pool of applicants who were given the opportunity to pitch to government agency heads in a bid to procure work, which many participants went on to do.[1]

[1] AustCyber (2022)

2 Export

Export Australian cyber security to the world

AustCyber provides resources, incentives and support to encourage Australian cyber security firms to export their products and services.

Some examples include:

- **Trade delegations**
  Australian cyber security firms, as well as related governments and academic organisations, have made 129 visits to six countries as part of our trade delegations.
- **Pitching events**
  AustCyber has organised nine pitching events since its inception. These events involve cyber security firms pitching their ideas to governments, sector experts and academics.
- **Export revenue**
  Australia's cyber security sector has increased its export revenue by $2.7 billion since AustCyber's inception in 2017.

3 Educate

Make Australia the leading centre for cyber security education

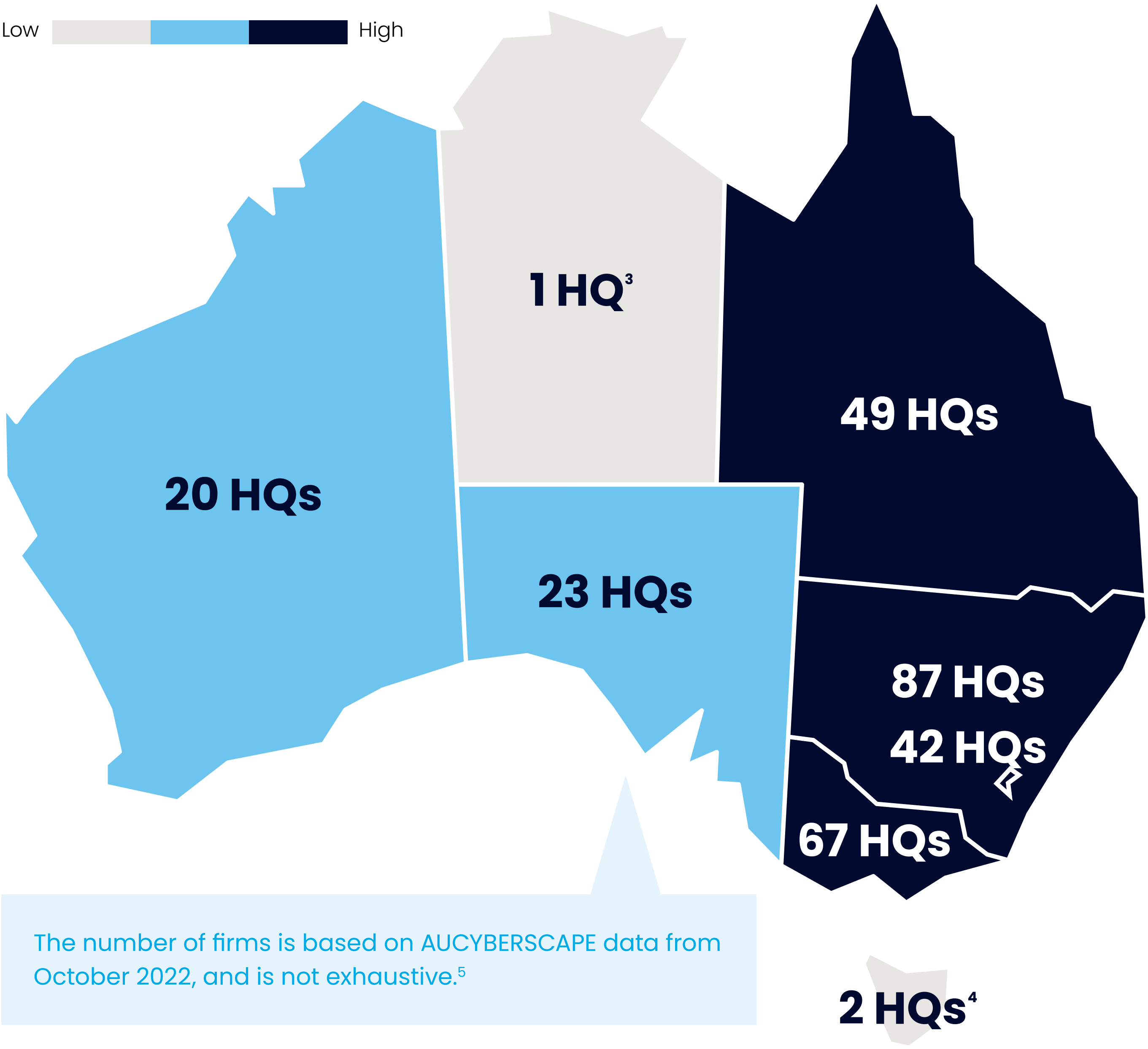
AustCyber directly and indirectly supports Australia's development into a leading centre for cyber security education.

Some initiatives include:

- **Cyber Week**
  During Cyber Week, AustCyber provides free training to participants. Over 1,000 people completed the free open-source intelligence (OSINT) training during Cyber Week 2021, with more due to complete it during Cyber Week 2022.
- **Education map**
  AustCyber developed an online interactive dashboard featuring Australian university and TAFE cyber security, information technology, and computer science programs available by provider location, course type, and duration to make education that may lead to a career in cyber security more accessible.
- **CyberCamp program**
  In 2019, AustCyber contributed to the development of a 20-hour cyber security curriculum for Australian schools, which aimed to inspire students to pursue studies in science, technology, engineering and mathematics (STEM).

There are 291 cyber security firms in Australia, with almost 85 per cent located in the eastern states

Exhibit 1: State-by-state snapshot of Australia's cyber security firms on AUCYBERSCAPE as at 28 October 2022[2]



The number of firms is based on AUCYBERSCAPE data from October 2022, and is not exhaustive.[5]

[2] AustCyber's Digital Census 2022. The number of headquarters in each state is sourced from AUCYBERSCAPE data as of 28 October 2022 and is not exhaustive. The actual number of cyber security providers in Australia is expected to be much higher, approximately 350. Figures are not comparable to those published in the 2020 SCP. Median firm age, percentage of firms less than five years old and exporting figures are based on cumulative data from AUCYBERSCAPE and updated responses captured in AustCyber's Digital Census 2022.

[3] A snapshot has not been provided for the Northern Territory as it only has once cyber security firm – Digitalshield.

[4] A snapshot has not been provided for Tasmania as it only has two cyber security firms in the state, Blackheart Cyber Security and The Project Lab.

[5] AUCYBERSCAPE (2022), Accenture analysis

Western Australia	
Median firm age	5
Percentage of firms <5 years old	25%
Percentage of firms that export	44%

South Australia	
Median firm age	9
Percentage of firms <5 years old	29%
Percentage of firms that export	29%

Victoria	
Median firm age	5
Percentage of firms <5 years old	47%
Percentage of firms that export	52%

Queensland	
Median firm age	7
Percentage of firms <5 years old	35%
Percentage of firms that export	47%

New South Wales	
Median firm age	5.5
Percentage of firms <5 years old	34%
Percentage of firms that export	58%

Australian Capital Territory	
Median firm age	5
Percentage of firms <5 years old	38%
Percentage of firms that export	56%

Australia-wide

Median firm age

5

percentage of firms <5 years old

36%

percentage of firms that export

50%

Australia’s cyber security sector will generate an estimated $2.4 billion of Gross Value Added (GVA) in 2022, up from $2.2 billion in 2020

The Australian cyber security sector will generate an estimated $2.4 billion in GVA for the 2022 calendar year. GVA is a measure of economic activity used to estimate the contribution of the cyber security sector to Australia’s GDP. It is the sum of the gross operating surplus and wages in the sector. The 2022 GVA figure is comprised of 37.5 per cent wages and 62.5 per cent gross operating surplus.

Australia’s cyber security sector GVA has grown by 11 per cent over two years. This is faster than growth in the healthcare and social assistance sector and the financial services sector.[6] The growth since 2020 is a result of increased awareness of cyber security risks and higher rates of digitisation increasing the need for cyber security.

The economic contribution of the Australian cyber security sector is not limited to the profits and wages it supports. Cyber security also plays a critical role in enabling economic activity in other sectors. For example, industries such as banking, technology and telecommunications would not be able to conduct their business without robust cyber security capabilities.

Exhibit 2: Estimated gross value added by Australia’s cyber security sector[6]

GVA (direct)

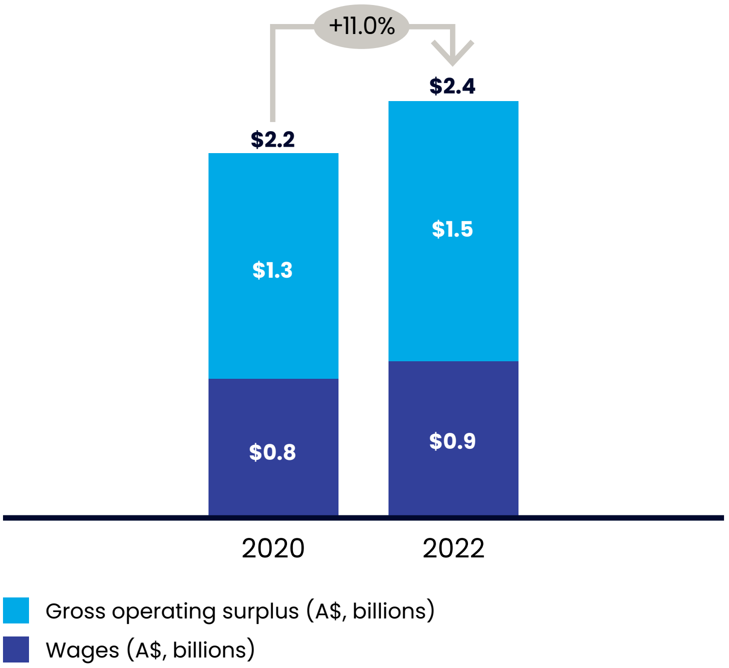
GVA (direct) is estimated by adding operating profits and wages for each calendar year. This estimate does not include indirect economic impacts.

Gross operating surplus

Gross operating surplus estimate is based on data from more than 80 respondents in AustCyber’s Digital Census 2022, scaled to account for sector size, as well as ABS data and public company reports.[8]

Wages

Total sector wages are estimated by applying a weighted average wages to revenue ratio from the Digital Census to Australian cyber sector revenue, as well as ABS data.[9]



[6] ABS National Accounts (2022)
[7] Figures are not comparable to those published in the 2020 SCP due to a re-baselining of data.
[8] AustCyber’s Digital Census is AustCyber’s sector survey used to inform components of the SCP.
[9] Gartner Information Security Forecast, Worldwide, 2016–2026, 1Q22 Update, Accenture analysis.

Almost 47,000 people work in cyber security in Australia, outpacing other high-value sectors including medtech and renewable energy

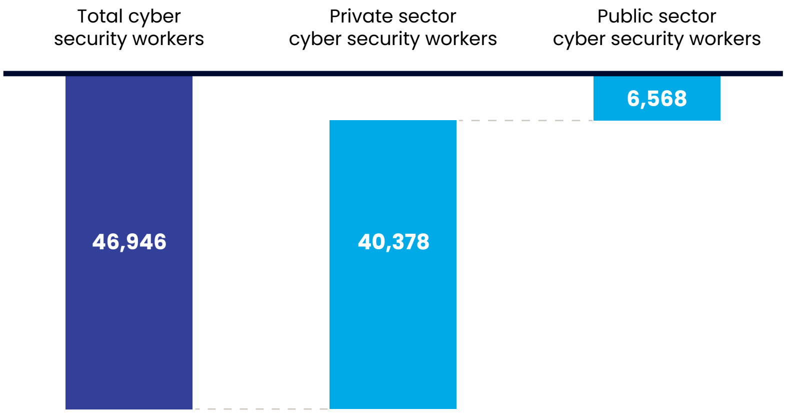
The cyber security sector employs almost 47,000 people in Australia today. The cyber security workforce includes full-time, part-time, and contractor employees, in dedicated roles only. Dedicated cyber security workers are those whose job titles reflect a pure cyber security position, such as a Cyber Security Engineer or an Information Security Analyst. Cyber security workers in related roles (all other jobs which require cyber security skills and expertise, regardless of job title) account for an additional 96,700 workers but are not included in these figures. The high number of related roles indicates a growing need for cyber security skills more broadly.

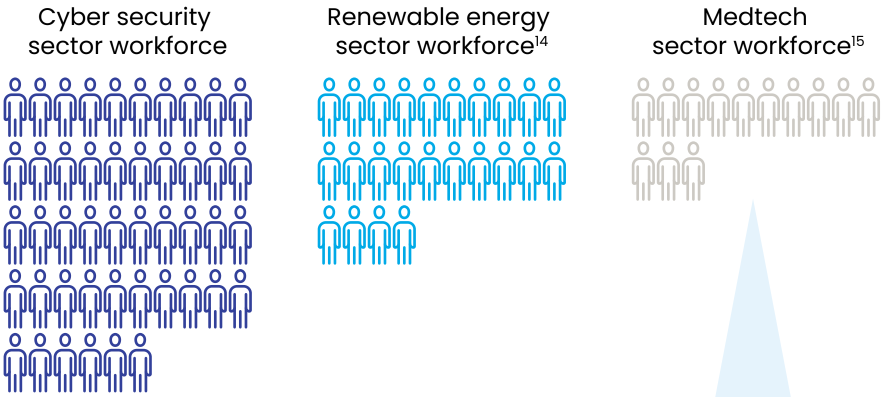
Private sector employment makes up 86 per cent of the cyber security workforce, with the remaining 14 per cent employed by the public sector. Cyber security sector employment split between the private and public sector is in line with total national employment, where 85 per cent of the population work for the private sector and 15 per cent work for the public sector.

The cyber security sector supports further employment by enabling the digital economy. The cyber security sector has a much greater impact on Australia's overall employment through related jobs, as well as indirect jobs, as it underpins the digitisation and growth of the entire economy.

Exhibit 3: Australia cyber security workforce[10,11]

Number of workers in FY22, thousands





The cyber security sector is strong, currently **employing approximately 3.5 times more than the medtech sector**, which has been identified as one of Australia's six priority manufacturing areas selected to grow high-value skills and jobs.[15]

[10] ABS Employment and Earnings, Public Sector (2021)
[11] Figures are not comparable to those published in the 2020 SCP due to a new methodology for estimating the size of the cyber security workforce, using AUCyberExplorer data.
[12] According to most recent data (2018–19)
[13] AUCyberExplorer 2022
[14] ABS Employment in Renewable Energy Activities (2020)
[15] ABS Australian Industry Employment (2022), Accenture analysis

On average, Australia is hit by a cyber attack every two minutes, with experts expecting the number to double in the next five years

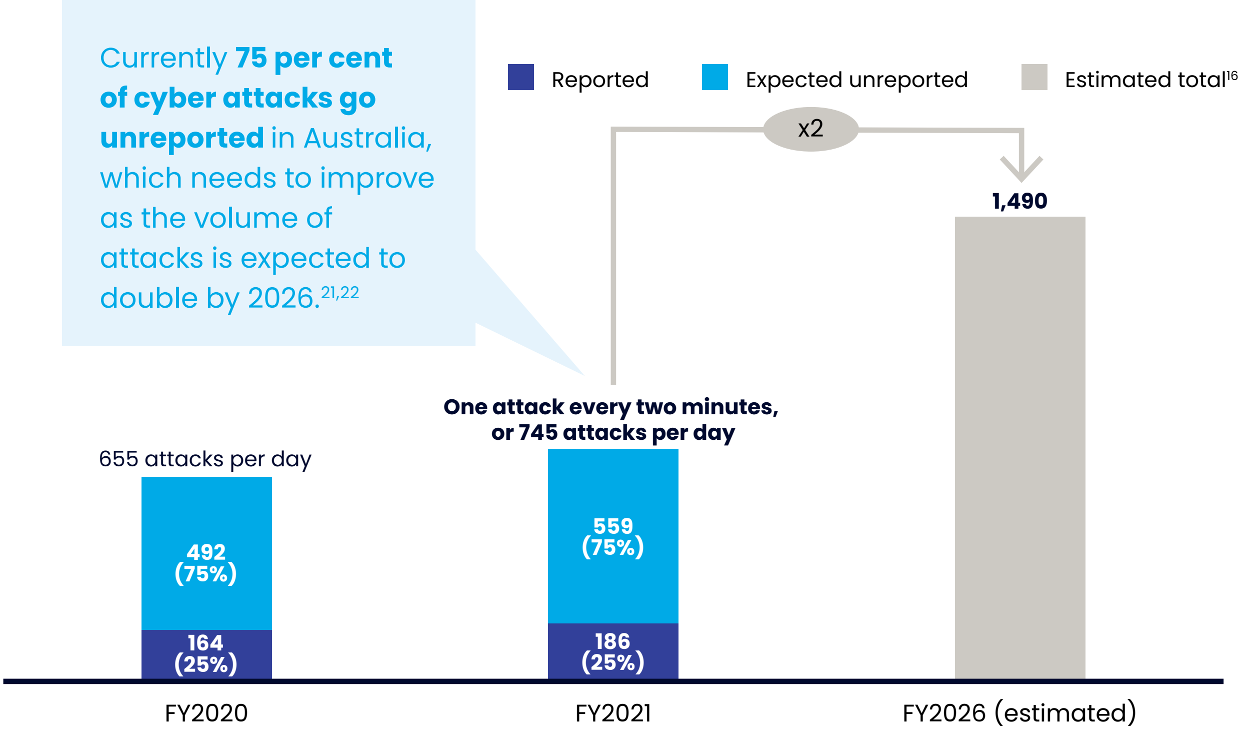
In 2021, Australia experienced 745 cyber attacks per day, or one every two minutes. This is 14 per cent more attacks than were reported in 2020. These figures are consistent with the global increase in cyber attacks. Since 2016, the average growth rate in cyber attacks is 15 per cent per year globally.[16]

According to AustCyber's Digital Census 2022, 75 per cent of cyber attacks against Australian organisations are not reported to the Australian Cyber Security Centre (ACSC). Until 2021, only governmental organisations were required to report cyber attacks to the ACSC under the Security of Critical Infrastructure (SOCI) Act. However, in 2021, the Act was extended from four to 11 industry groups, which will likely increase the number of attacks reported to the ACSC.[17]

Unreported cyber attacks decrease national security and can cause more severe disruption to victims.[19] The longer a cyber attack goes unresolved, the more costly it will be. Reporting cyber attacks often reduces the resolution time. The estimated cost increase of cyber attacks left unresolved for extended times ranges from 11 per cent to 35 per cent.[18, 19]

The number of cyber attacks is expected to double over the next five years.[20] Experts believe that geopolitical tensions and ransomware will be the key drivers of an increasing number of attacks.[23]

Exhibit 4: Number of cyber attacks in Australia



[16] AustCyber's Digital Census 2022 – "In your opinion, what percentage of cyber attacks go unreported in Australia?
[17] Home affairs (2021)
[18] IBM (2021)
[19] Accenture (2021)
[20] Cyber Security Ventures (2022)
[21] Australian Cyber Security Centre (2022)
[22] Consultancy (2022)
[23] Expert interviews, Accenture analysis

The most commonly reported attacks are low-level malicious attacks, and the most common targets are governments and large organisations

The Australian Cyber Security Centre (ACSC) uses a framework to categorise cyber attacks. The ACSC categorises cyber attacks by severity based on the type of attack (rows) and targeted organisation (columns). The ACSC then determines its response and resource allocation based on the severity (indicated by shading) of the cyber attack.

Low-level malicious attacks, such as phishing and targeted scanning, are the most frequently reported cyber attacks. More than half of reported cyber attacks in Australia are low-level malicious attacks. Phishing attacks are the most reported type of low-level malicious attack. In a phishing attack, cyber criminals send people a malicious link to obtain personal information.

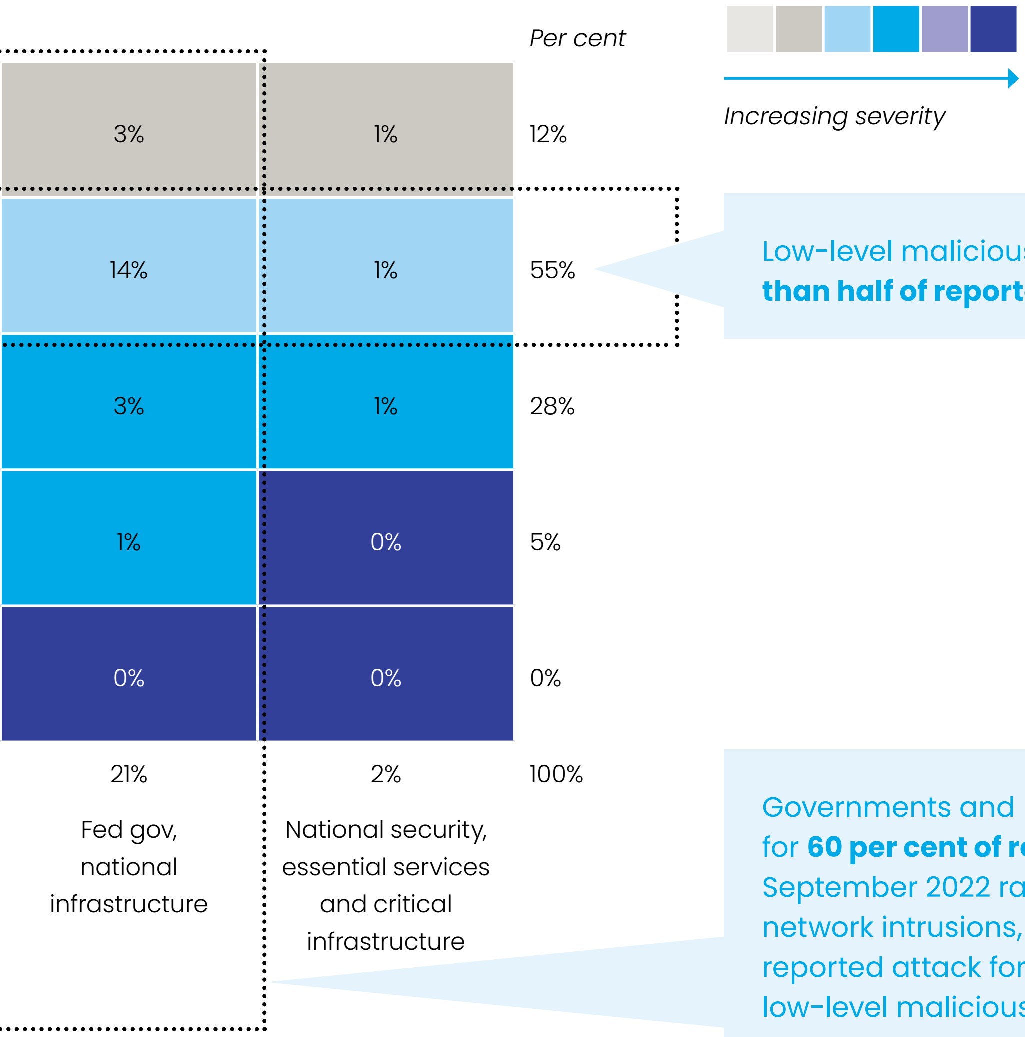
Exhibit 5: Number of reported cyber attacks in Australia, by scenario and severity[24,25,26,27,28]
Percentage of reported cyber attacks per year actioned by ACSC, FY2021

Cyber attack or scenario				
Scanning or reconnaissance	1%	1%	1%	6%
Low-level malicious attack – phishing, targeted scanning	4%	5%	12%	19%
Active network intrusion – malware, beaconing or other	0%	5%	7%	13%
Exfiltration or deletion/damage of key sensitive data or IP	0%	1%	1%	2%
Sustained disruption of essential systems and associated services	0%	0%	0%	0%
Per cent	5%	11%	22%	39%
Target organisation:	Members of the public	Small organisations	Medium-sized organisations	State gov, large organisations

[24] Number of reported attacks likely underreported, and shifted to governmental organisations, due to mandatory reporting.
[25] Percentages might not add up due to rounding.
[26] HBR (2021)
[27] Australian Cyber Security Centre (2022)
[28] Heimdal (2022), Accenture analysis

Governments and large organisations report the most cyber attacks. Governmental organisations represent a high proportion of reported attacks in part because they are required to report cyber attacks to the ACSC.

Large organisations are also frequently targeted because a successful attack against a large organisation could create greater windfalls for malicious actors whose focus is on obtaining sensitive company information and intellectual property. Alternatively, they target large organisations with ransomware to encrypt their system and demand ransom payments.[24]



Fed gov, national infrastructure	National security, essential services and critical infrastructure	*Per cent*
3%	1%	12%
14%	1%	55%
3%	1%	28%
1%	0%	5%
0%	0%	0%
21%	2%	100%

Low-level malicious attacks account for **more than half of reported attacks**.

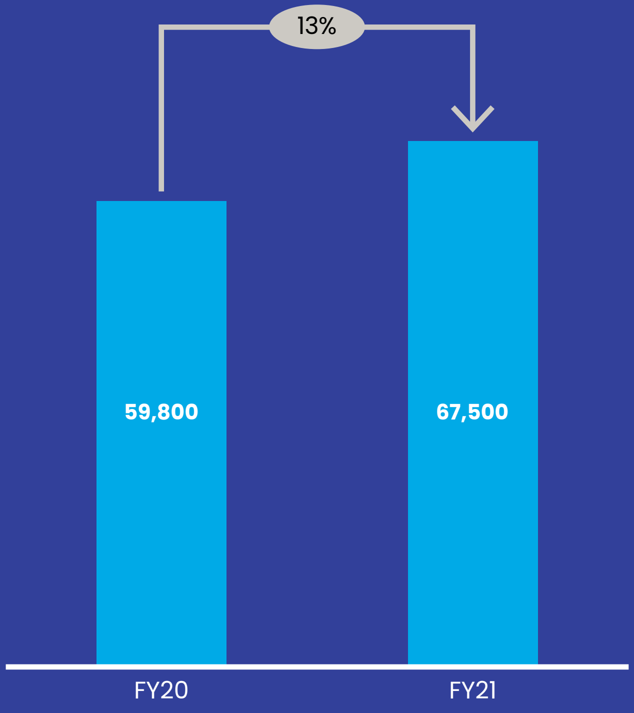
Governments and large organisations account for **60 per cent of reported cyber attacks**. The September 2022 ransomware attacks are active network intrusions, which is the second most reported attack for large organisations, after low-level malicious attacks.

Case Study

The number of cyber attacks against Australian companies increased by 13 per cent between FY20–21 and appears to be continuing to rise

The number of cyber attacks in Australia is rising sharply[29]

Number of cyber attacks reported to ACSC



Telecommunications

A recent ransomware attack on a large telecommunications provider has been flagged as the worst in Australian history, threatening almost 10 million customers' information – impacting the equivalent of 40 per cent of the Australian population. The hackers demanded a payment of US$1 million in cryptocurrency, which the provider declined to pay. Instead, the telecommunications provider is working with the Australian government to prevent data from being leaked on the dark web.

The costs of this attack include expenses on increased cyber security capability, legal support, customer compensation, fines and long-term profitability losses. The costs to the broader economy are high and still largely unknown, as the additional threat of dark web data sales and potential further scams and hacks is imminent. Identity theft and the long-term financial impacts on victims' credit scores, borrowing power and more are also a key concern. **This attack highlights the role cyber security plays in protecting value created in the economy and the importance of threat detection and corrective action measures.**

[29] Australian Cyber Security Centre (2022)

Retail

A major online retailer suffered a cyber attack affecting up to 2.2 million customers' data, including names, dates of birth, addresses and phone numbers. The firm is working alongside the Office of the Australian Information Commissioner (OAIC) to investigate the attack and keep customers adequately informed. **The management of this case demonstrates the benefit of working with authorities to manage cyber attacks.**

Banking

The names and email addresses of employees of a big four bank were accessed by hackers. The bank claimed the data was accessed "through a third-party provider for an employee and member benefits program – this is not a breach of our systems".[2] The bank is continuing to monitor the risks and impacts of the breach. **The third-party nature of this data breach serves as a reminder that cyber security risk exists across the economy, and national efforts to increase cyber security uptake are imperative.**

A cyber attack against Australia could cost up to $12.6 billion

Attack scenario

An active network intrusion via Log4j where financially driven malicious actors exploit the Log4j vulnerability to obtain access to computers and networks, wherefore they gain access to victims' data and confidential files. Affected firms would be unable to use their digital infrastructure, causing huge disruption and economic losses. The impacts would vary between industries, for instance, retail businesses may not be able to buy or sell goods online, while information technology firms may have to shut down their entire operation until the breach is rectified.

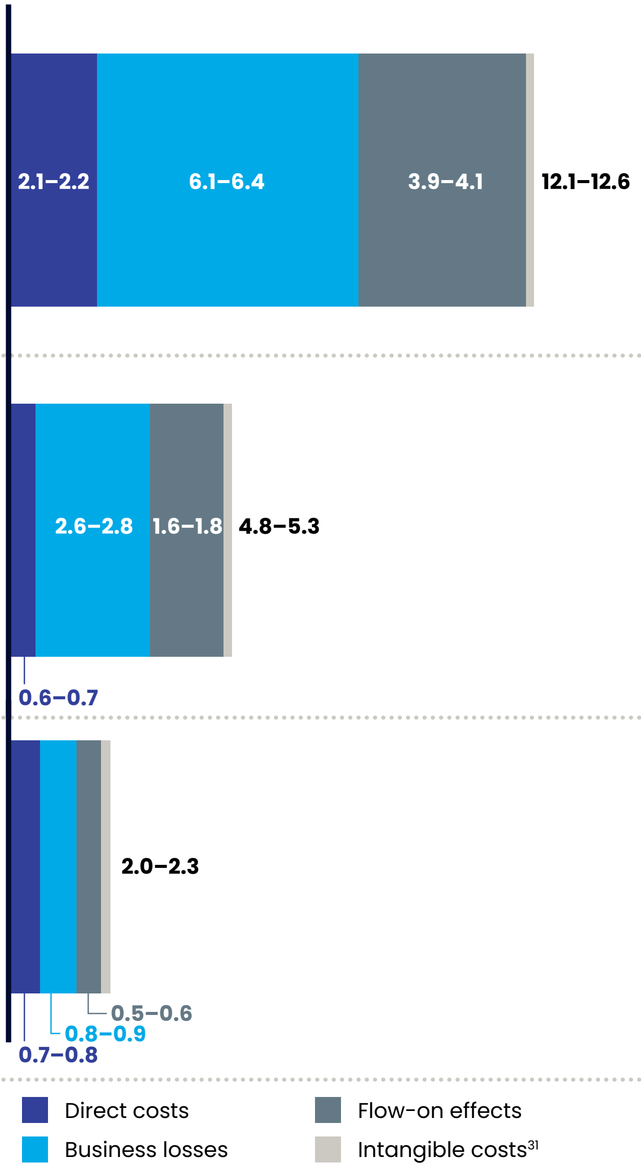
A sustained disruption to the electricity grid where state actors attack the IT infrastructure of an Australian electricity provider, leading to a blackout across New South Wales. All households and businesses in New South Wales would be impacted by the electricity outage, experiencing downtime. This is conservative, as an attack to the National Electricity Market (NEM), which connects the entire east coast of Australia, could cause blackouts across five states.[34]

A widescale low-level malicious attack where malicious actors coordinate widescale phishing attacks to obtain personal information and data. Up to 60 per cent of businesses would be affected, as well as millions of households. Impacted businesses risk sensitive information being accessed and would need to update information like back account details.

[30] The Australian (2022)
[31] AustCyber's Digital Census 2022
[32] Computer Weekly (2021)
[33] Kaspersky (2022)
[34] Guardian (2022)
[35] Trellix (2022)
[36] ABC (2022)
[37] Technology Review (2022)
[38] ACSC (2022)
[39] ACCC (2022)

Exhibit 6: Potential cyber attack cost

A$ billions



Why this scenario?

- Up to 60 per cent of firms in Australia have a Log4j vulnerability, making this scenario devastating.[31] The Log4j vulnerability is already being exploited by malicious actors; over 93 million Log4j-related attacks were detected in 2021.[32]
- In 2017, a widescale attack using the WannaCry ransomware infected 230,000 systems and is estimated to have cost US$4 billion globally.[33]

- Australia's grid is increasingly vulnerable to hackers as the electricity system becomes more complex.[35,36]
- A similar attack occurred in 2022 in Ukraine. The Ukrainian electricity grid was attacked by Russian hackers, which could have led to an outage for two million people.[37]

- Phishing attacks are the most reported type of cyber attack in Australia.[38] 71,000 reports of phishing attacks were made to the ACCC in 2021.[39] Direct financial costs of phishing attacks have quadrupled between 2017 and 2021.[39]
- Phishing attacks are on the rise, with malicious actors taking advantage of health scares during COVID-19 to distribute phishing scams.

02
Australian cyber security sector growth is slower than peers for three reasons

Australia's cyber sector annual revenue growth has averaged 8.7 per cent over the past five years – slower than other leading cyber jurisdictions

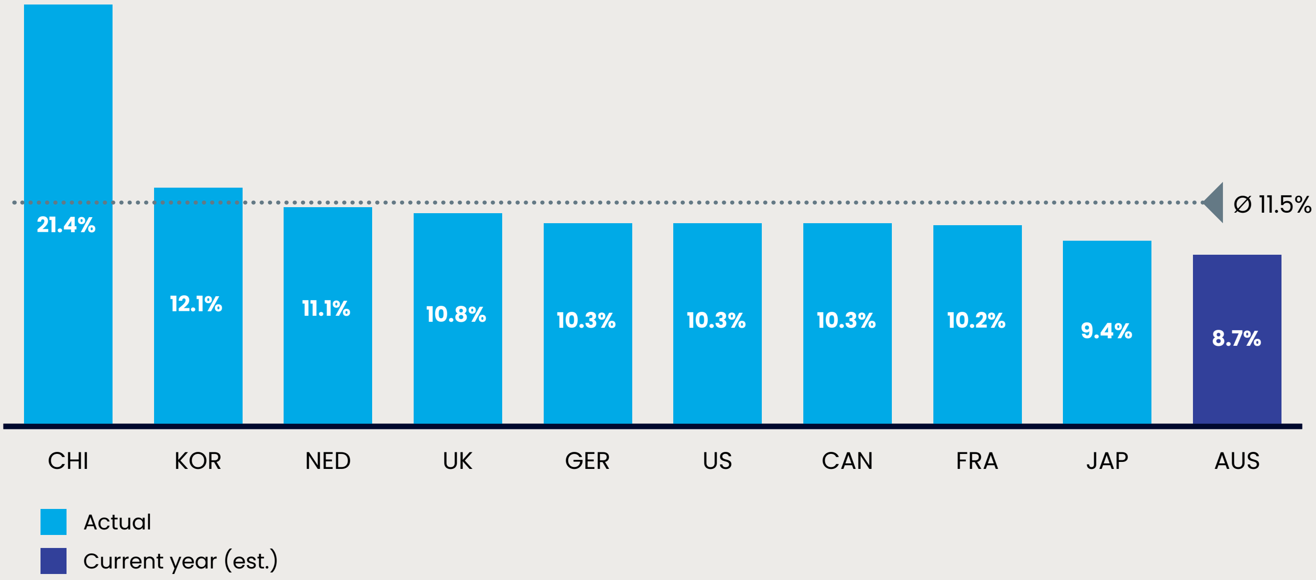
The Australian cyber sector's revenue growth has been slower than other leading nations. Australian firms' annual revenue growth has averaged 8.7 per cent since 2017. The average growth rate for the 10 leading cyber jurisdictions (based on 2022 revenue) has been 11.5 per cent. Chinese cyber firms' revenue growth has been the strongest of all leading nations at 21.4 per cent.

External tensions, ecosystem benefits and strict regulations have contributed to strong growth in leading jurisdictions. Countries such as China and South Korea have invested heavily in their cyber sector driven by an increased focus on sovereignty due to political tensions. Cyber firms in the Netherlands have benefitted from a strong digital ecosystem supported by the government. The Hague is home to the Global Forum on Cyber Expertise, Europol's European Cybercrime Centre, the NATO Communications and Information Agency and The Hague Security Delta, the largest security cluster in Europe. The cyber sector in the UK has benefitted from the EU's General Data Protection Regulation (GDPR), retained in the UK post-Brexit, that enacts some of the strictest penalties for data breaches (up to 20 million euros or four per cent of turnover – whichever is greater).[1,2]

In 2022, Australia is ranked ninth globally in terms of revenue. The US has the greatest share of global revenue, followed by China, the UK, Japan, Germany, France, Canada, South Korea, Australia and the Netherlands.

Exhibit 7: Growth rates of largest cyber jurisdictions[3,4,5]

Average annual revenue growth rate between 2017 and 2022 (%) of top 10 cyber jurisdictions based on 2022 revenue



[1] International Trade Administration (2021)
[2] GDPR (2022)
[3] Gartner Information Security Forecast, Worldwide, 2016–2026, 1Q22 Update
[4] McKinsey (2020)
[5] Statista (2022), Accenture analysis

Australian cyber security sector growth is slower than international peers for three reasons

Ranking

1 Limited startup support	2 Insufficient focus on export markets	3 Workforce shortages
Investment into cyber security startups[7]	*Domestic share of cyber security demand*[8]	*Percentage of bachelor students enrolled in ICT*[6,9]
1. Singapore	1. US	1. Ireland
2. Israel	2. UK	2. New Zealand
3. Estonia	3. Japan	3. Iceland
4. US	4. Germany	4. Finland
...	...	...
15. Australia	**8. Australia**	**23. Australia**

[6] OECD countries and direct peers (Singapore and South Korea) are included in rankings. Enrolments in ICT degrees is used as a proxy for cyber security, in absence of cyber security specific data. Leading countries are based on FY22 figures and as such, may not align to those outlined in Exhibit 7, which are measured over the 2017–2022 period.
[7] Crunchbase (2022)
[8] Gartner Information Security Forecast, Worldwide, 2016–2026, 1Q22 Update
[9] OECD (2022), Accenture analysis

Australian cyber security startups receive 300 times less funding than peer leaders

Australian startups generate less value in early-stage funding than international competitors. In 2022, Australian startups received 300 times less funding than Israeli and Canadian startups. As a result, they have less ability to scale.

Australia's venture capital ecosystem is immature compared to peer countries.[10] Australia has a small venture capital market compared to international peers. Australia ranks 20th out of 38 OECD countries in venture capital funding as share of GDP, lower than Israel, Canada and Singapore.[11] Government funds in Israel and Canada have supported strong investment in both countries. The preparedness to invest in early startups further decreased during COVID-19, evidenced by a decline in investments characterised by higher uncertainty.[11]

Cyber security firms consider the lack of funding a key challenge. When asked about challenges the sector faces in AustCyber's Digital Census 2022, respondents highlighted funding as a significant barrier to growth.

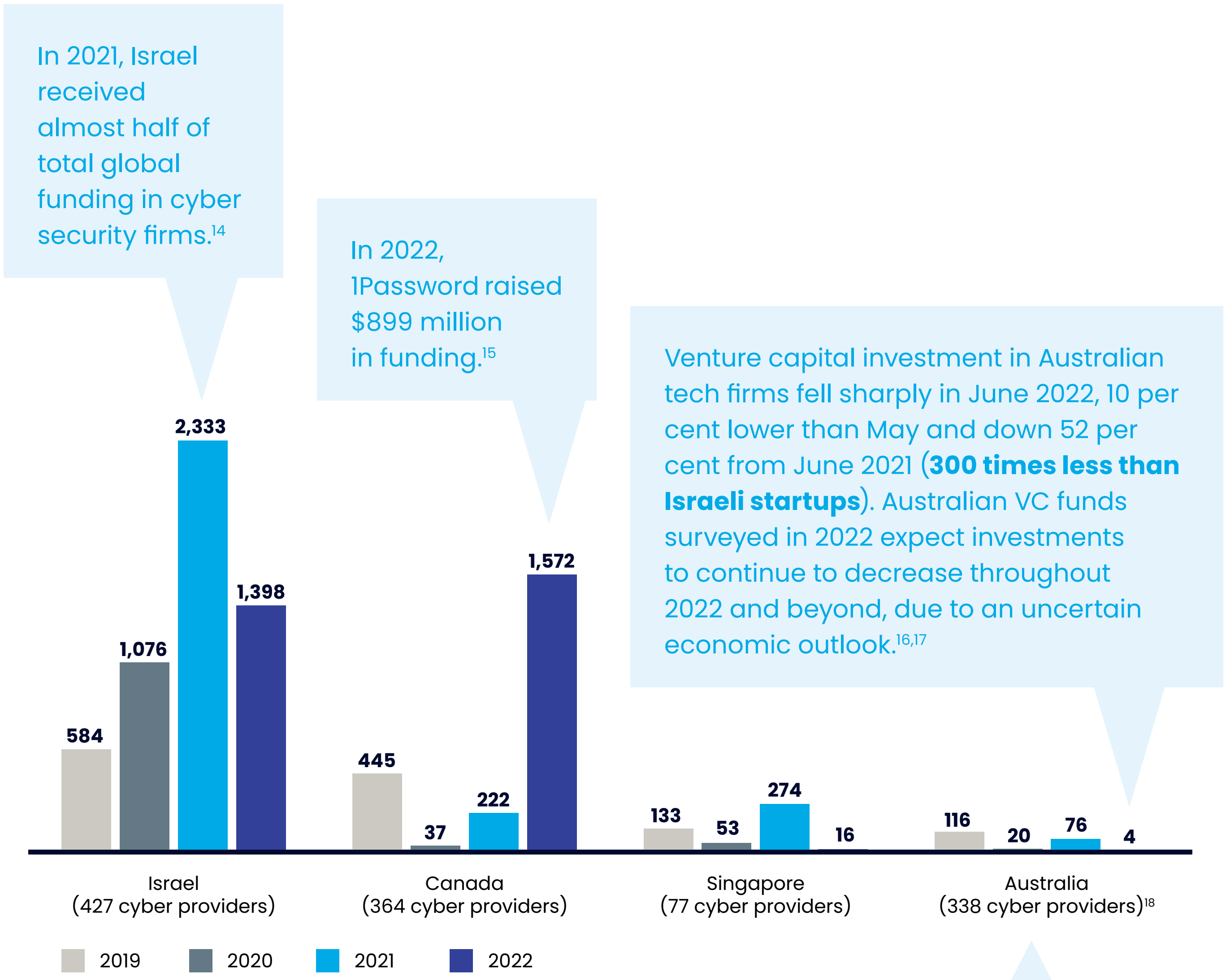
> "Lack of investment is a key challenge for us to go from a healthy seed-round as expected by our Series-A potential investor."

> "[Australian cyber security organisations have] difficulty scaling due to low capital and no relevant grant opportunities."

[10] Blackbird Ventures (2021)
[11] OECD (2021)

Exhibit 8: Value of early-stage funding rounds[12,13]

A$ million



In 2021, Israel received almost half of total global funding in cyber security firms.[14]

In 2022, 1Password raised $899 million in funding.[15]

Venture capital investment in Australian tech firms fell sharply in June 2022, 10 per cent lower than May and down 52 per cent from June 2021 (**300 times less than Israeli startups**). Australian VC funds surveyed in 2022 expect investments to continue to decrease throughout 2022 and beyond, due to an uncertain economic outlook.[16,17]

Since 2019, Australian cyber security firms have raised less than half (45 per cent) the capital than their Singaporean counterparts have, even though there are almost five times as many firms in Australia.

[12] 2022 figures include investments made between Jan and June.
[13] 'Cyber security firms' based on Crunchbase's reported data, which captures a broader range of firms than AUCYBERSCAPE.
[14] Haaretz (2022)
[15] Crunchbase (2022)
[16] AFR (2022)
[17] AFR (2022)
[18] Expert interviews, Accenture analysis

Cyber security research funding has decreased by 23 per cent since 2019 due to consecutive decreases in ARC funding

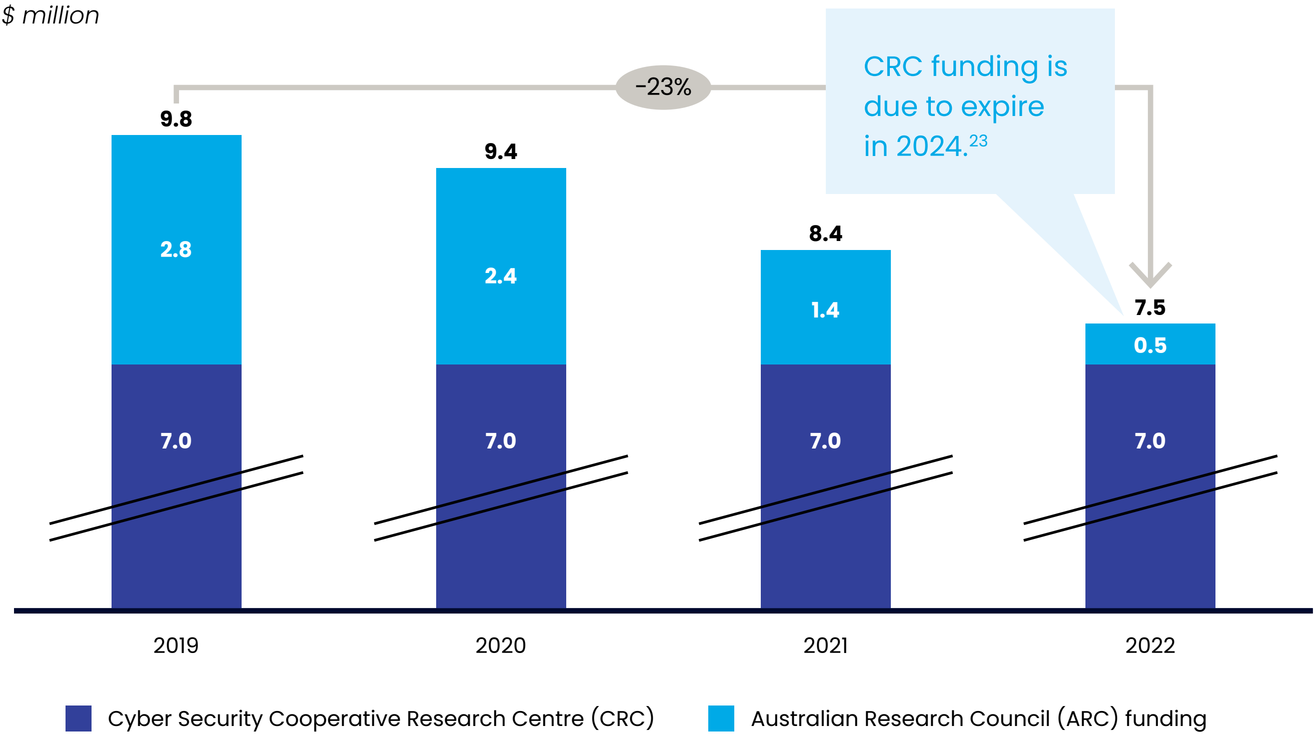
Cyber security research funding has decreased by 23 per cent since 2019. Funding has reduced due to consecutive annual decreases in Australian Research Council (ARC) funding. ARC funding has decreased by $2.3 million since 2019, with just $500,000 being distributed in 2022.[19]

Cyber security attracts less research funding than similar research fields. In 2022, ARC allocated over $10 million in research funding to artificial intelligence, more than 20 times more funding than cyber security. In the same year, machine learning received $1.1 million research funding from ARC, twice the amount directed to cyber security. Sector experts suggested that the relatively low funding for cyber security from the ARC could be due to limited cyber security expertise and awareness among ARC grant assessors.

Currently, the Cyber Security Cooperative Research Centre (CSCRC) provides 93 per cent of cyber security research. CSCRC funding is due to expire in 2024, which, if not extended or replaced, would reduce government funding for cyber security to almost zero, based on current trends. The CSCRC is the sector's central research organisation and has a long-term focus on critical infrastructure security and cyber security as a service.[20] It has more than 20 partners from industry, government and research, including six leading Australian universities, all of which contribute funding.

Exhibit 9: Government funding directed to cyber security research[21,22]

A$ million



[19] ARC figures include both Discovery and Linkage projects and include total funding announced for 2022. CSCRC figures are based on $50 million of government funding over the seven years to 2024.
[20] Individual funding from the CSCRC's members is not included as this is not classified as government funding.
[21] Funding includes money allocated to universities or other research institutions.
[22] Australian Research Council (2022)
[23] Cyber Security Cooperative Research Centre (2022), Accenture analysis

As a result of limited startup support in the form of investment and research funding, the rate of new firm entries in cyber security has slowed in recent years

Australia's cyber security sector has seen years of rapid growth. Between 2014 and 2019, the number of businesses in the cyber security sector grew by more than 10 per cent each year, more than three times higher than the broader economy or the comparable IMT sector.

There has been a slowdown in the entrance rate of new cyber security startups over the past two years. The growth rate in new businesses has decreased from 22 per cent in 2019 to six per cent in 2021, according AustCyber's Digital Census 2022.

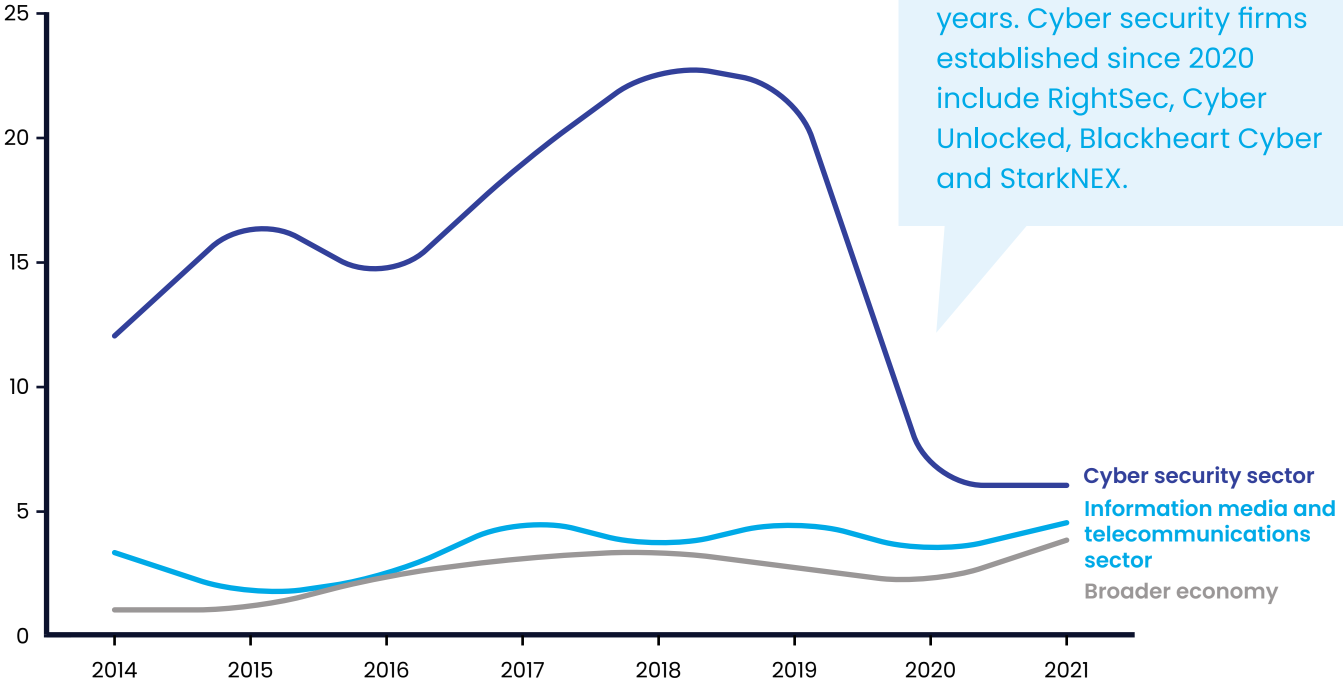
The decline in growth is likely due to limited early stage funding and a period of economic uncertainty during COVID-19. The Australian cyber security sector has a low level of early-stage funding compared to international peers, and funding in 2020 and 2021 was lower than 2019, which has likely impacted the growth rate in the number of firms in the sector. Additional economic uncertainty from 2020 as the pandemic ensued may also have impacted the entry rate of cyber security startups.

Although growth has slowed, there is still strong activity in the startup space. 13 per cent of cyber security firms in Australia were established in 2020. Examples include RightSec, CyberUnlocked, Blackheart Cyber and StarkNEX.

2022 survey data indicates 13 per cent of Australian cyber security firms were established in the last 2 years. Cyber security firms established since 2020 include RightSec, Cyber Unlocked, Blackheart Cyber and StarkNEX.

Exhibit 10: Growth rate in number of firms by sector[24,25,26]

Percentage per year



[24] Analysis is based on AustCyber's Digital Census 2022 data, which – due to sample composition – might understate recent growth.

[25] AustCyber's Digital Census 2022 "When was your organisation established?"

[26] ABS (2022), Accenture analysis

Australian cyber security firms derive less revenue from export than other comparable international firms

Australian cyber security firms do not receive a significant share of revenue from exports. The Australian cyber security sector receives approximately 17 per cent of its revenue from exports currently, less than half of the UK's 42 per cent share.[27]

Cyber security products and services are well-suited to exporting. The cross-border nature of cyber security threats supports a global market for security solutions. Australian products and services are applicable in most markets, presenting a strong opportunity for exports.[27]

Increasingly, Australian firms are facing competition from overseas. Not only is global competitiveness important for growing revenue but also for protecting existing domestic revenue. According to the AustCyber's Digital Census 2022, 53 per cent of Australian firms report their main competitors are international firms. Sector experts suggested that firms targeting organisations in critical infrastructure face strong competition from international firms.[28]

Exhibit 11: Percentage of firms exporting in Australia and the UK

Percentage of survey respondents

Only 42 per cent of Australian cyber security firms export their products and services, nine per cent less than UK cyber security firms.

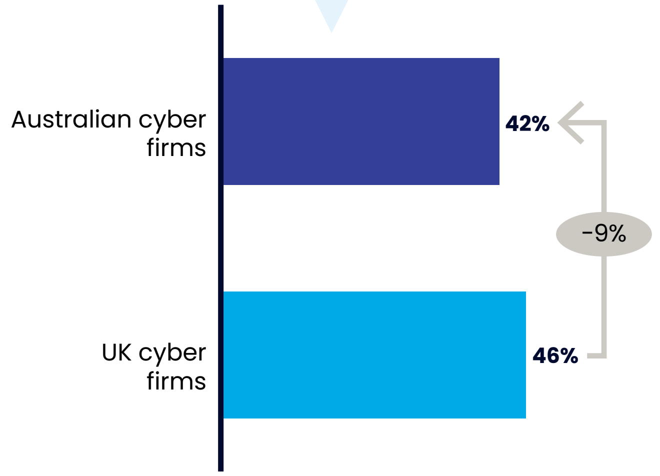
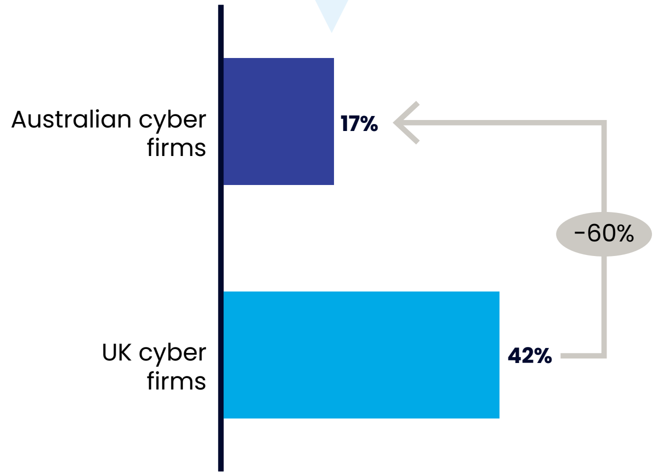


Exhibit 12: Share of Australian and UK sector revenue from exports[28,29]

Percentage of 2022 revenue, by source

Australian cyber security firms create 60 per cent less revenue from exporting, compared to UK firms.



[27] UK Government (2021)
[28] Expert interviews, Accenture analysis
[29] AustCyber's Digital Census 2022 – "Throughout the 2021/22 financial year, has your organisation exported (or will your organisation export) any products and/or service? Who are your main competitors?"

Focusing on serving local demand offers fewer opportunities, as Australian cyber security expenditure represents only 2.1 per cent of global demand

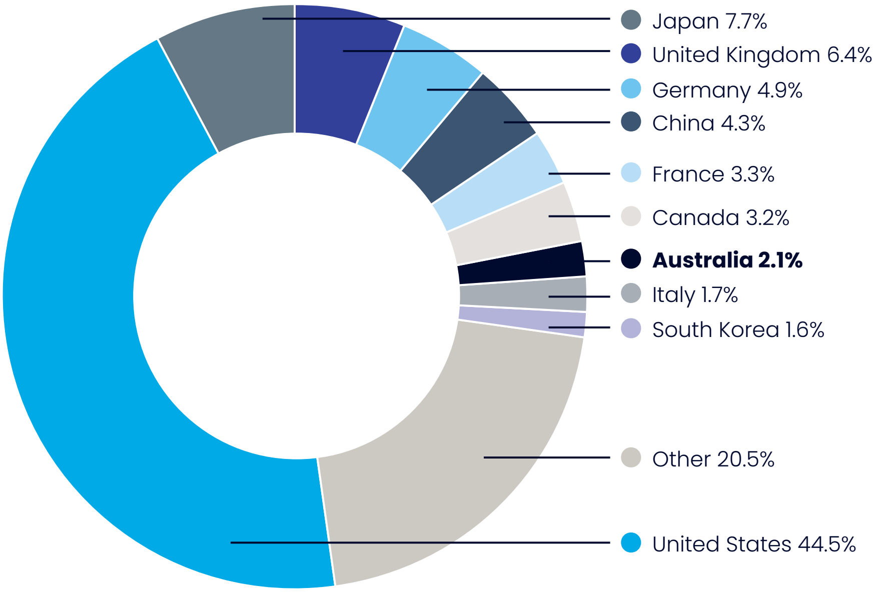
Australia accounts for only 2.1 per cent of global cyber security demand. Australia's domestic demand ranks eighth globally. The US has the greatest share of global cyber security expenditure, followed by Japan, the UK, Germany, China, France and Canada.

Australia's domestic demand has been gradually declining and is forecast to continue to decline. Australia's share of global cyber security expenditure is 2.1 per cent in 2022. The share is down from 2.2 per cent in 2017 and is forecast to further decline to 1.9 per cent by 2025.

Australian cyber security firms that only focus on the domestic market have a small serviceable market. Australian cyber security firms need to expand overseas to achieve scale.

Exhibit 13: Cyber security expenditure by country[30]

Share of global cyber security expenditure, 2022 (%)



Australia's share of demand has been gradually declining and is forecast to continue to decline. An opportunity exist to expand overseas markets to achieve scale.

[30] Gartner Information Security Forecast, Worldwide, 2016–2026, 1Q22 Update, Statista (2022), Accenture analysis

Workforce shortages are further handbrakes on growth, with the sector forecast to have 3,000 fewer cyber security workers than required by 2026

Australia's cyber security sector is expected to have 3,000 fewer workers than required by 2026, despite projected growth of 1,200 workers over the period. Demand for cyber security workers will increase to 51,100 workers by 2026. However, based on projected inflows and outflows from the cyber security workforce, by 2026 there will be a shortage of 3,000 workers. Only 48,100 of the demanded roles will be filled.

Between 2022 and 2026, it is expected that 9,500 current cyber security workers will leave the workforce. This figure includes workers retiring from the workforce and those moving to other industries. This estimate is based on the exit rate for the broader ICT sector.

8,300 new cyber security workers and 2,400 skilled migrants are expected to join the Australian cyber security workforce by 2026. Together, new graduates, upskilled and reskilled workers and skilled migrants will more than replace workers leaving the workforce. This means that there will be an increase of 1,200 workers to the Australian cyber security workforce by 2026.

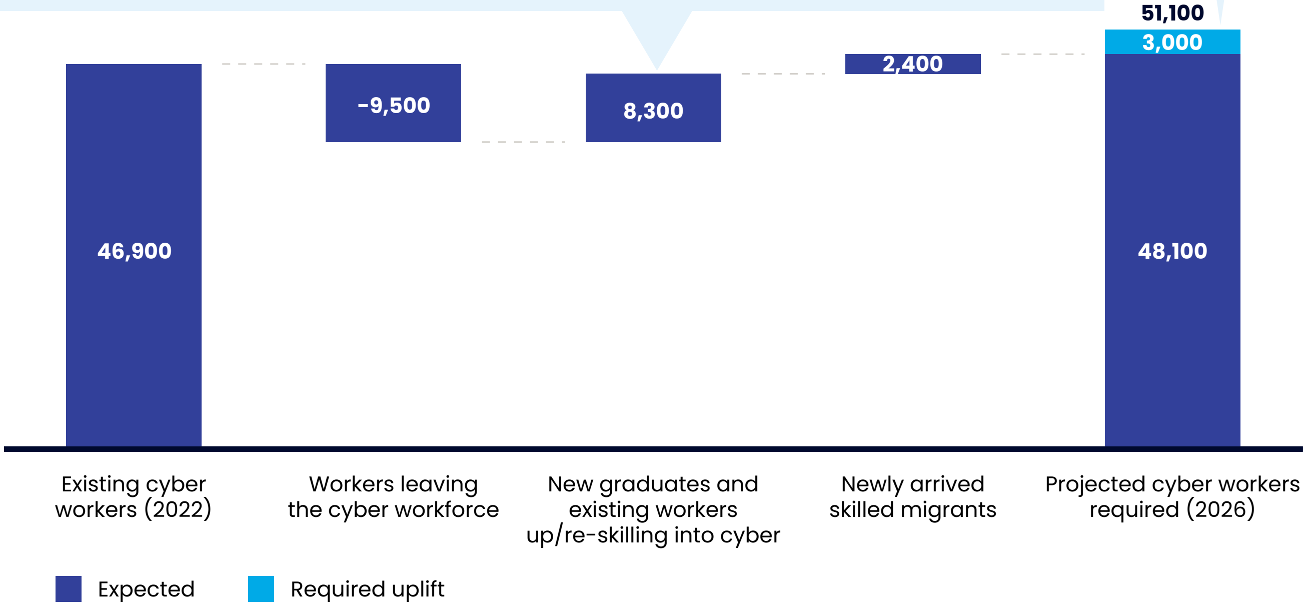
These results are based on AUCyberExplorer estimates of sector employment. Estimates are not comparable to those published in the 2020 SCP, where employment estimates were derived from revenue and value added.

Australia will have 3,000 fewer cyber security workers than demanded by 2026, unless further action is taken.

Exhibit 14: Cyber security workforce forecast[31,32]

Number of cyber security workers 2022–2026

Only five per cent of skilled migrant visas are granted to cyber security workers, compared to 21 per cent in MedTech, despite the sector being smaller. Australia should look to increase migration numbers for cyber security specialists to support the growth requirements of the sector by 2026.[33]



[31] See Appendix A.4 for detailed methodology. Figures are not comparable to those published in the 2020 SCP due to a changed methodology and changed data sources.
[32] AUCyberExplorer (2022)
[33] Deloitte Digital Pulse (2022)

The workforce shortage is partially a result of lower migration, with the number of skilled visas granted in tech almost halved since FY19

Skilled visas for tech occupations have declined by 49 per cent between 2019 and 2021, contributing to the skills shortage. Australia has historically relied on skilled migrants to support the tech and cyber security workforce.[34] To achieve sectoral growth, the cyber security sector requires 3,100 skilled migrants over the next four years. Border closures during COVID-19 significantly reduced tech and cyber security skilled migration.

Skilled migration is expected to return to above pre-pandemic levels by 2026. Migration is expected to fully return to pre-COVID levels in 2025.[35] However, there is currently a backlog of more than 140,000 skilled migrant visas.[36] Processing times for skilled visas have doubled since COVID-19. A quarter of applications now take more than a year to process, and the slowest 10 per cent of skilled visas take 15 months to process.[37]

Despite being one of seven priority sectors, only 5 per cent of all visas issued across these seven priority sectors in 2021 were for cyber security workers. Australia's Global Talent Program aims to attract highly skilled professionals in seven priority sectors to Australia. These sectors are information and communications technology, energy and mining tech, medtech, fintech, advanced manufacturing, agritech and cyber security. The number of visas granted for cyber security skilled workers was lower than any other sector.

Increasing skilled migration of cyber security workers is essential. Attracting experienced cyber security workers from overseas will be vital to reducing the skills gap, particularly for experienced professionals. Expert interviews revealed that many firms face a shortage of mid to senior-level cyber security professionals, which are difficult to attract domestically.

[34] Deloitte Digital Pulse (2022)
[35] ABC (2021)
[36] Department of Home Affairs (2022)
[37] AFR (2022)

Exhibit 15: Supply of skilled visas for all tech occupations[38]

'000s, number of skilled visas granted for tech occupations

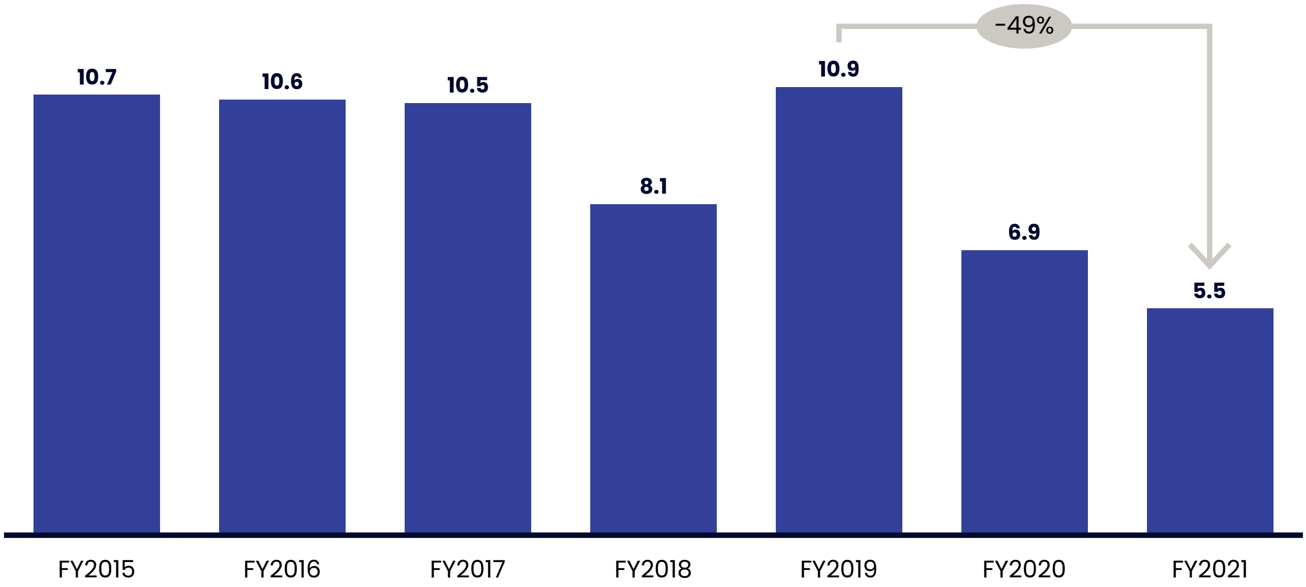
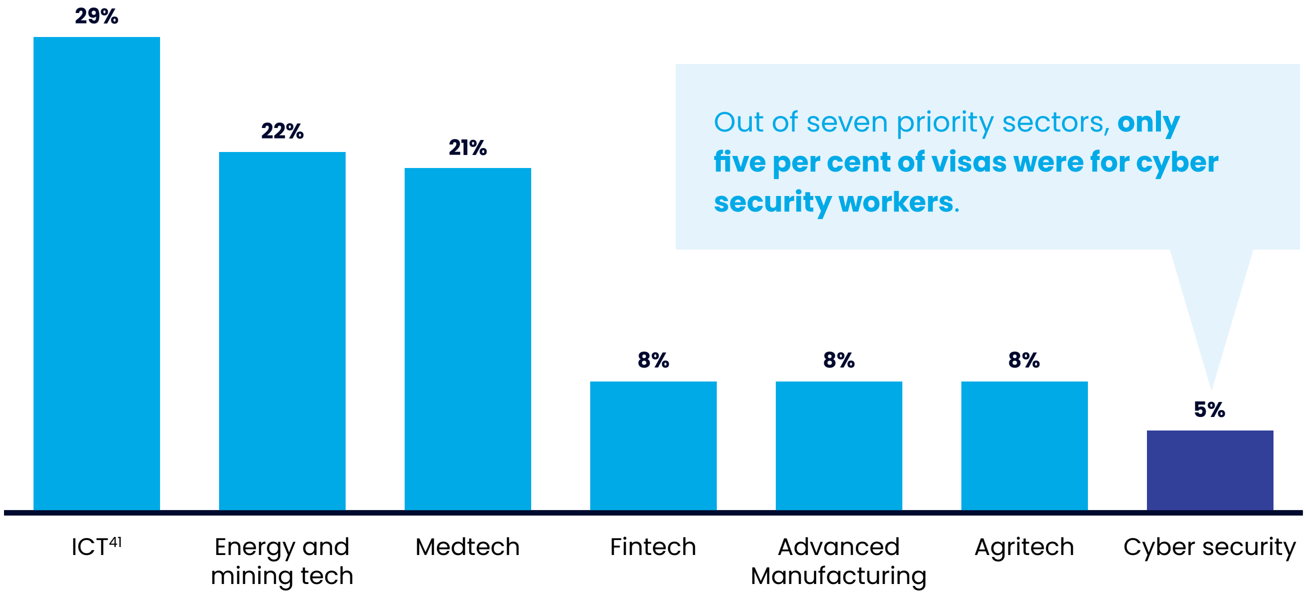


Exhibit 16: Skilled visas granted to priority sectors[39,42]

Percentage of granted Global Talent skilled visas granted by priority sectors[40]



Out of seven priority sectors, **only five per cent of visas were for cyber security workers**.

[38] See Appendix for detailed methodology.
[39] The Australian Government has selected future-focused priority sectors to promote immigration of highly skilled talent to Australia (Visa subclass includes 186, 187, 482, 494 and 858).
[40] Priority sectors represent a subset of all tech occupations
[41] ICT includes Quantum Information, Advanced Digital, Data Science.
[42] Grattan Institute (2021), Accenture analysis

03 Australia has an opportunity to add $800 million to annual cyber security revenue by 2026 through three key actions

If Australia acts on the identified growth barriers, the cyber security sector will move up the leaderboard, potentially earning $800 million more annually by 2026

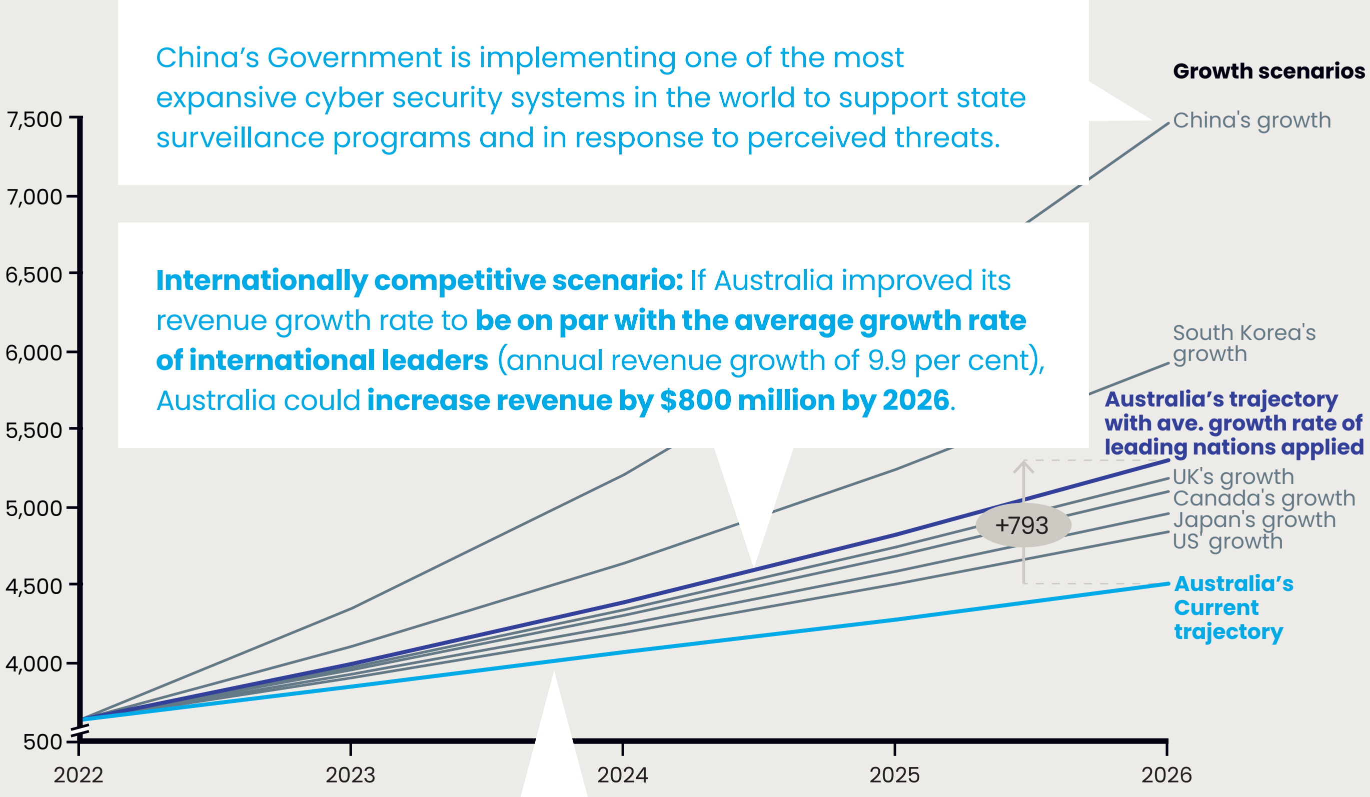
The Australian cyber security sector has an opportunity to increase its annual revenue by $800 million. If Australia improved its revenue growth rate to be on par with the forecast annual average growth rate of international leaders (9.9 per cent), Australia could increase its annual cyber security revenue by $800 million by 2026.

Australia’s annual revenue growth is forecast to be 5.5 per cent, while the average of leading cyber security jurisdictions is forecast to be 9.9 per cent. Of the top 10 cyber security jurisdictions (based on 2022 revenue), China is forecast to have the strongest annual growth by 2026, at 19.7 per cent. South Korea has the second highest at 13 per cent. Australia has the lowest forecast annual growth rate, at 5.5 per cent.

To grow revenue, Australia must improve its startup environment, bolster domestic procurement and export capability and better attract local and international talent. This report finds that these three impediments are slowing Australia’s cyber security sector growth relative to peers.

Exhibit 17: Australia’s modelled revenue under various scenarios

Australia’s revenue A$, millions



China’s Government is implementing one of the most expansive cyber security systems in the world to support state surveillance programs and in response to perceived threats.

Internationally competitive scenario: If Australia improved its revenue growth rate to **be on par with the average growth rate of international leaders** (annual revenue growth of 9.9 per cent), Australia could **increase revenue by $800 million by 2026**.

On Australia’s **current trajectory** (annual revenue growth of 5.5 per cent), Australia is forecast to **lose 15 per cent market share** between 2022 and 2026.

Australia has an opportunity to add $800 million to annual cyber security revenue by 2026 through three key actions

Key actions

1

Support research, innovation and startup development

Support and incentivise cyber security research and development

Support the innovation ecosystem

2

Bolster domestic procurement and export capability

Support domestic procurement of cyber security for governments and SMEs

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

3

Attract local and international talent

Offer competitive remuneration and fast-track skilled visa applications to attract talent

Expand technology education and upskill and reskill current workers

Increase incentives and funding for R&D, as well as support the innovation ecosystem, to address the challenge of limited startup support

⚫ Government ⚪ Educators 🔵 Cyber security firms

Policy objective			
Support and incentivise cyber security research and development		Support the innovation ecosystem	
Recommendation			
- **Increase R&D funding from the Australian Research Council** to match peer economies, such as Israel, the United States and Singapore. Increasing R&D funding to universities will boost innovation and creation.	- Continue to **refine and illustrate the scope and clarity of R&D tax incentives** for software development to promote R&D in sector.	- Build on the success of AustCyber's Australian Cyber Week. Continue **collaboration between businesses and educators** and promote the development and early adoption of advanced technologies via innovation hubs.	- **Continue to mature the innovation hubs** by coordinating sector engagements and aligning policies to sector needs.
International example			
🇮🇱	🇩🇪	🇬🇧	🇸🇬
- Israel has the world's highest R&D expenditure; 4.9 per cent of national GDP. Australia's R&D expenditure is less than half of Israel's, at 1.8 per cent of GDP. - Experts suggest that Israel's R&D expenditure has allowed it to become a global leader in innovation, having some of the highest rates of scientific articles and patents per capita.[4] Israel has developed a strong ICT sector, which accounts for approximately 20 per cent of GDP.[5]	- Germany has developed specific software tax incentives for firms working on software development, where firms can claim up to 25 per cent of R&D expenses per year. - The tax incentives were introduced in 2020 to support digital innovation and strengthen the domestic technology sector.[6]	- The UK's Catapult Network is a government-led initiative to foster collaboration between businesses and academia by building better connected, collaborative ecosystems. - The program had resulted in more than 4,000 academic collaborations and 15,000 sector collaborations between 2013 and 2021.[7]	- Singapore's Infocomm Media Development Authority (IMDA) is a statutory board in the Singapore government. It supports development of the information technology sector by connecting startups with multinationals. - IMDA's strategic partner program has supported partnerships between Singaporean tech companies and multinationals, such as Apple, IBM, Microsoft, Samsung.[8]
Responsible			
⚫	⚫	⚫🔵	⚫🔵

[1] Gartner Information Security Forecast, Worldwide, 2016–2026, 1Q22 Update
[2] CSIS (2022)
[3] Statista (2022), Accenture analysis
[4] WIPO (2021)
[5] OECD (2022)
[6] German Government (2020)
[7] UK Government (2021)
[8] Singapore Government (2022), Accenture analysis

Support domestic procurement of cyber security, alongside continuing efforts to grow exports, thereby providing a broad base of growth

● Government ◍ Educators 🔵 Cyber security firms

Policy objective	Support domestic procurement of cyber security for governments and SMEs		Maintain and strengthen the sector's global, export-oriented outlook	
Recommendation	• **Continue to improve government procurement systems** to support procurement from domestic cyber security firms.	• **Grow the domestic cyber security market** by supporting SMEs with cyber security education and cyber security implementation.	• **Maintain strong government support** for the cyber security sector by supporting AustCyber's and Austrade's trade delegations. Provide market research publications, training and introductions to customers.	• **Support entrepreneurs to visit Silicon Valley,** to provide them with valuable entrepreneurial experience in the California tech hub.
International example	🇳🇱	🇸🇮	🇺🇸	🇯🇵
	• The Netherlands Government has implemented procurement processes to prioritise domestic cyber security firms. • As a result of the updated procurement process, the Netherlands Defence force now works together with a Netherlands-European consortium of technology firms for all their cyber security services.[9]	• Slovenia provides vouchers to SMEs for cyber security, providing up to 60 per cent of total cyber security costs offered by specific contractors. • Over 1,000 businesses have used a voucher to purchase cyber security services. SMEs reported that the voucher system was user-friendly and encouraged businesses to take cyber security measures.[10]	• The US International Trade Administration provides trade missions specifically designed for companies who want to travel to target countries. These missions include networking events, briefings and training opportunities. • Businesses in ICT have demonstrated interest in more missions to seek opportunities in global tech hubs.[11]	• Japan has announced plans to send 1,000 entrepreneurs and business development executives to Silicon Valley over the next five years. • These visits are designed to enable Japanese entrepreneurs to learn from their Silicon Valley counterparts – particularly with regards to the "not afraid to fail" mentality.[12]
Responsible	●	●	●	● 🔵

[9] Netherlands Government (2022)
[10] Slovenian Government (2021)
[11] US Government (2021)
[12] Japan Times (2021), Accenture analysis

Work together on attracting talent and upskilling workers to take the handbrakes off the Australian cyber security sector growth

⚫ Government ⚪ Educators 🔵 Cyber security firms

Policy objective	Offer competitive remuneration and fast-track skilled visa applications to attract talent			Expand technology education and upskill and reskill current workers	
Recommendation	• Maintain attractiveness of the sector as an employer by **offering competitive wages via employee-share-programs.**	• Support international talent to relocate to Australia by **fast-tracking skilled visas.** Skills programs are currently costly and with a long application process, limiting the pool of potential workers.	• Develop a strong **diversity and inclusion strategy** to recruit a diverse and inclusive workforce, focusing on women and underrepresented communities.	• Continue work from the National Skills Commission. Invest in future cyber security talent by **partnering with educational providers** through placements and work integrated experiences, research and innovation opportunities, and career opportunities.	• Build on the success of AustCyber's education map to provide information on cyber security education. Continue supporting clear and accessible pathways to **retain and upskill workers in the current workforce via VET and university offerings.**
International example	🇺🇸	🇨🇦	🇬🇧	🇮🇱	🇪🇺
	• The United States' Employee Stock Ownership Plans offers an attractive and easy way for companies to offer competitive remuneration.[13]	• Canada's Express Entry scheme offers fast-tracked visas for skilled workers, offering a processing time of just two weeks. • Since the Express Entry was established, 95 per cent of applicants have found employment and earn on average 20 per cent more than non-Express Entry applicants.[14]	• United Kingdom's new cyber security strategy specifically focuses on improving the diversity in the workforce, by increasing accessibility to skills programs.	• Israel's CyberSpark is the coordinating body to encourage joint academia and sector partnership and train talent. • CyberSpark connects students from Israeli and international universities to cyber security firms and provide them with relevant work experience.[15]	• The European Union created the Cybersecurity Higher Education Database (CYBERHEAD), to provide an overview of cyber security program offerings. • CYBERHEAD is the largest validated cyber security higher education database in Europe. It has been the main point of reference for all citizens looking to upskill in cyber security.[16]
Responsible	⚫ 🔵	⚫	🔵	⚫ 🔵	⚫ ⚪

[13] US Government (2020)
[14] Canada Government (2020)
[15] Israel Government (2020)
[16] EU Commission (2021), Accenture analysis

Appendices

A.1 State of the sector

Australian cyber security industry revenue has increased 52 per cent over the last five years to $3.7 billion in 2022

Cyber security sector revenue has continued to grow in Australia, reaching $3.7 billion in 2022. Since 2017, the sector's revenue has grown 52 per cent.

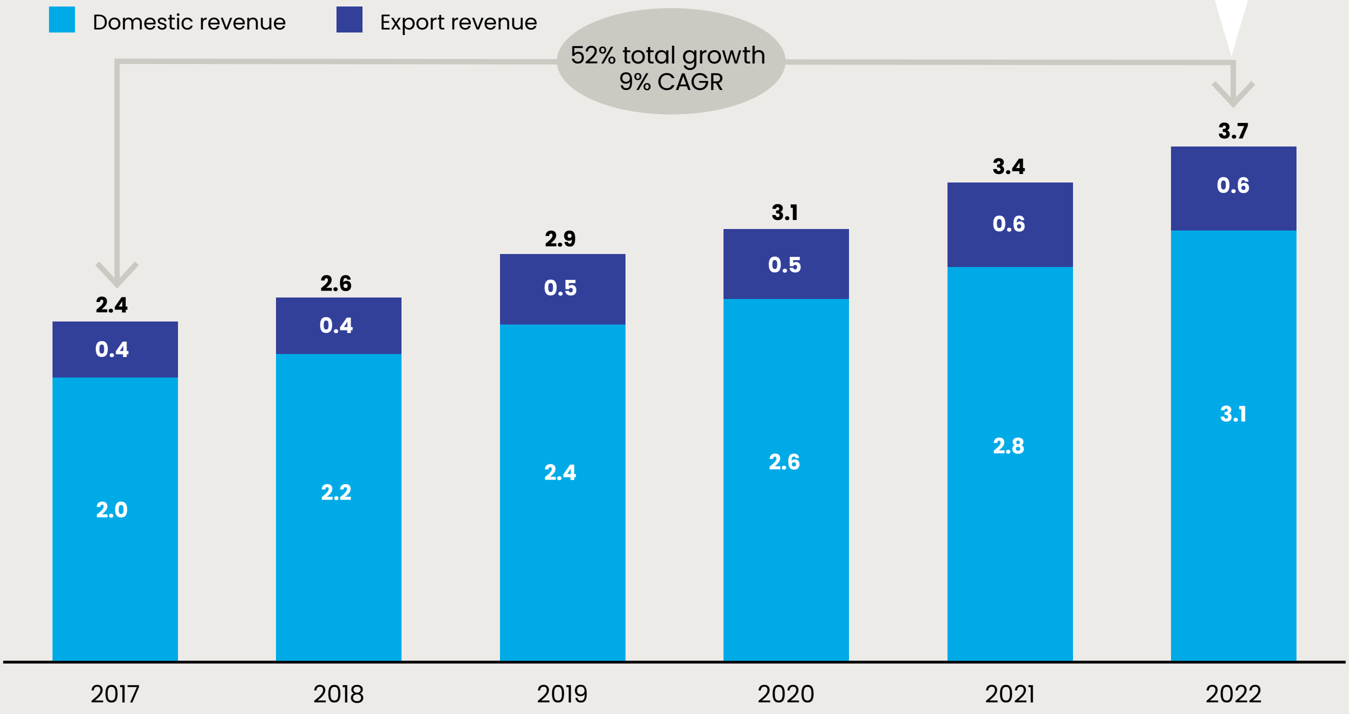
Revenue growth in Australia's cyber security industry has outpaced the broader Information Media and Telecommunications (IMT) industry. The Australian cyber security sector has seen a nine per cent compound annual growth rate (CAGR) over the past five years, while the broader IMT sector revenue in Australia grew at a CAGR of four per cent over the same period.[1]

83 per cent of revenue comes from the domestic market, with 17 per cent of revenue coming from overseas. Both domestic and export revenue have shown similar growth rates of approximately nine per cent from 2017 to 2022. Australian cyber security firms will sell an estimated $3.1 billion of goods and services to Australian buyers in 2022, up from $2.0 billion in 2017, and an estimated $600 million of goods and services to overseas buyers in 2022, up from $400 million in 2017.

Revenue growth is almost double that of the broader IMT industry, which has grown by about four per cent CAGR over the past 5 years.

Australia's cyber security sector revenue, 2017–22[3,4,5]

A$, billions



[1] ABS (2022)
[2] Figures are not comparable to those published in the 2020 SCP due to a re-baselining of data.
[3] Gartner Information Security Forecast, Worldwide, 2016–2026, 1Q22 Update
[4] IBIS World (2021)
[5] Austrade (2022), Accenture analysis

Government is the biggest consumer of Australian cyber security products and services

The government is the largest customer of Australian cyber security firms, accounting for 30 per cent of expenditure to Australian firms. Governments and their departments (including healthcare, social services, education and defence) are facing increased risks due to an increasingly complex threat landscape and a changing geopolitical outlook.

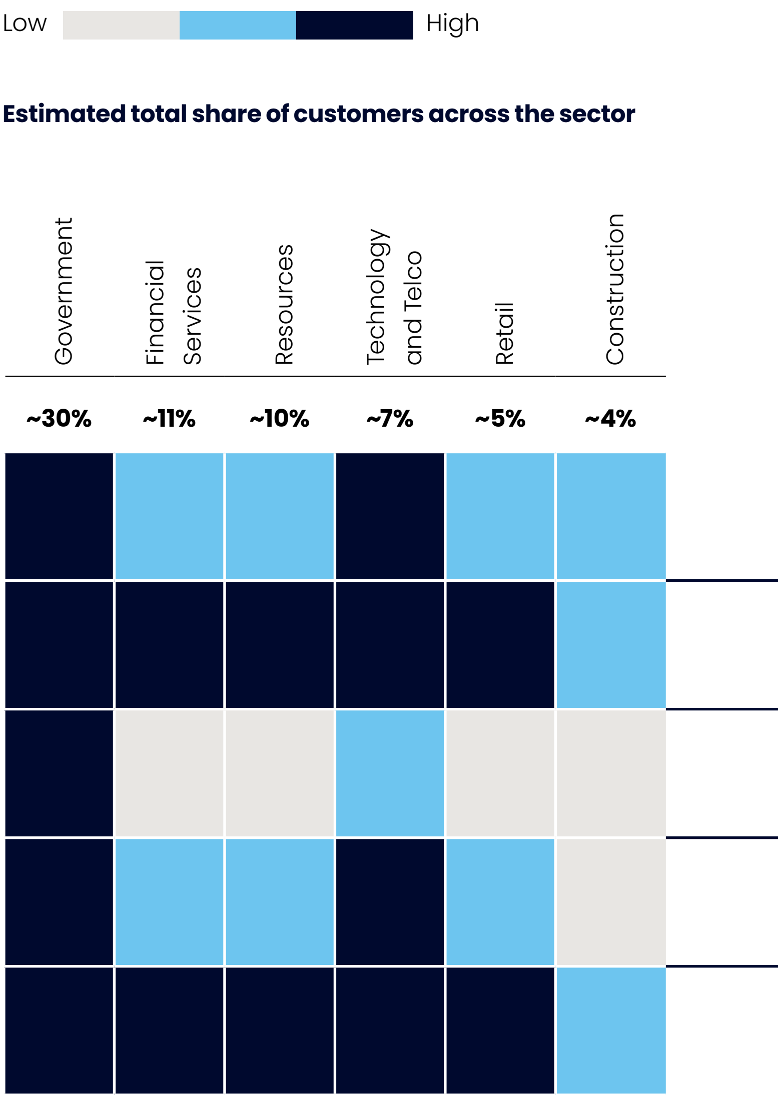
Financial services and resources are the second and third largest buyers of cyber security products and services. Financial services accounts for around 11 per cent of expenditure, while resources accounts for approximately 10 per cent. The top three customer groups comprise more than 50 per cent of total revenue in the sector in 2022.

Technology and telecommunications, retail and construction are the next three biggest cyber security customer groups in 2022, comprising less than 10 per cent of revenue each. All other industries serviced by Australia's cyber security sector account for less than five per cent of national revenue.

The Security of Critical Infrastructure (SOCI) Act could be contributing to increased spending in sectors covered by the Act. Sectors originally covered by SOCI Act 2018 include electricity, gas, water and maritime ports, and resources (which includes utilities). These are some of the largest cyber security customers in the nation. The 2022 amendment now includes 11 sectors. Because many entities such as those in government and financial services will likely be impacted by these reforms, this report expects spending in many sectors will also increase.

Australia's cyber security expenditure[6,7,8]

Expenditure to Australian firms by industry and product/service category



Low ⬜ 🟦 ⬛ High

Estimated total share of customers across the sector

Government	Financial Services	Resources	Technology and Telco	Retail	Construction
~30%	~11%	~10%	~7%	~5%	~4%
⬛	🟦	🟦	⬛	🟦	🟦
⬛	⬛	⬛	⬛	⬛	🟦
⬛	⬜	⬜	🟦	⬜	⬜
⬛	🟦	🟦	⬛	🟦	⬜
⬛	⬛	⬛	⬛	⬛	🟦

[6] AustCyber's Digital Census mostly captures SME providers so results have been supplemented to provide a more comprehensive view of the sector. High to low scale is across each product segment only.
[7] AustCyber's Digital Census 2022
[8] Expert interviews, Accenture analysis

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

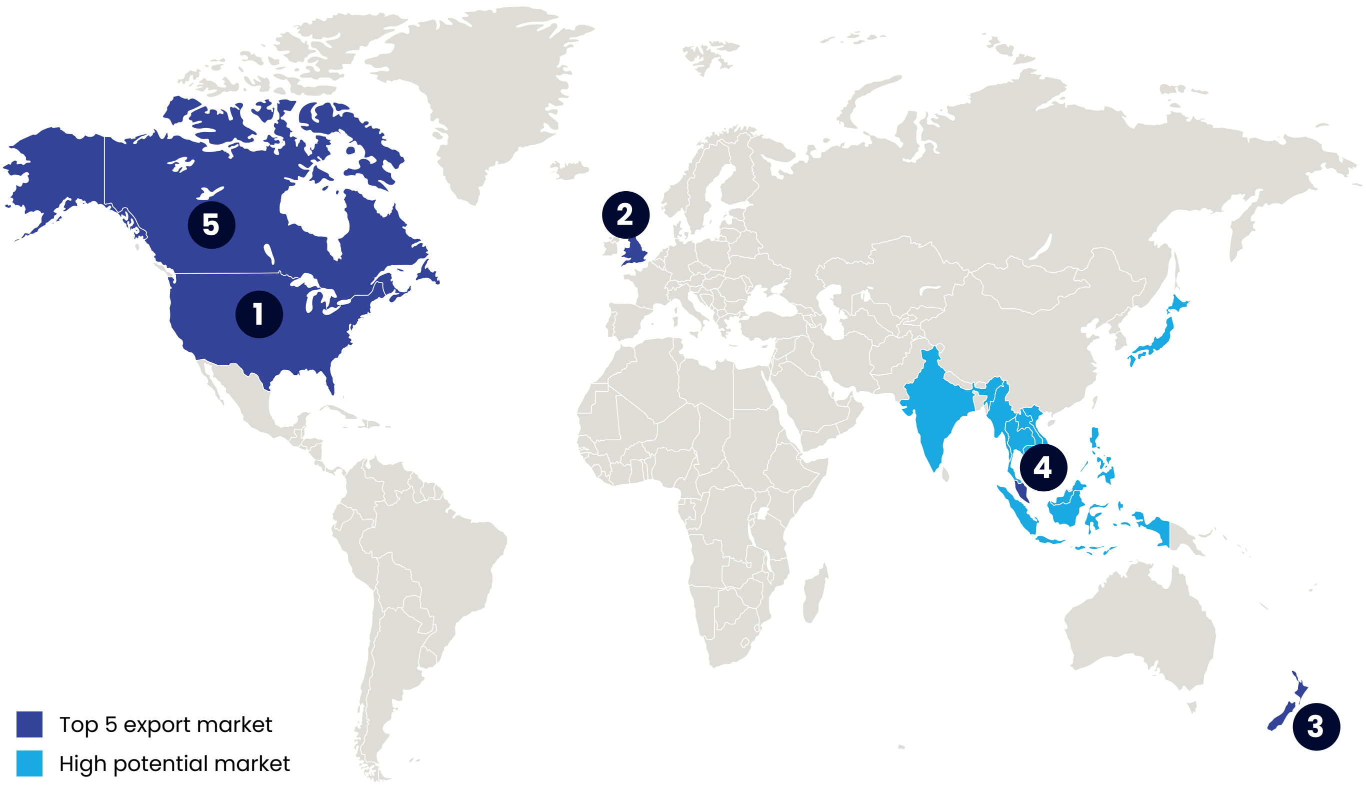
Infrastructure security: securing computer and digital networks and related physical hardware and systems against intruders

Software and platform security: security that focuses on keeping software and the entire computing platform and devices resilient to cyber security threats

Systems security: operational, network and systems security that includes the processes and decisions for handling and protecting data assets

The US, UK, New Zealand, Singapore and Canada are the most popular export markets for Australia's cyber security firms

Export destinations for Australian cyber security firms[9,10,11,12]



[9] List of export markets is based on AustCyber's Digital Census 2022, and as such, sample size may mean this list is not exhaustive.
[10] AustCyber's Digital Census 2022
[11] Australian High Commission (2020)
[12] Austrade (2021), Accenture analysis

1 US

82% of exporters export to the US

2 UK

57% of exporters export to the UK

3 New Zealand

39% of exporters export to New Zealand

4 Singapore

29% of exporters export to Singapore

5 Canada

18% of exporters export to Canada

India

Currently **attracts 11 per cent** of exporters. Growth is supported by the Australia-India Cyber and Critical Technology Partnership (AICCTP) grant aimed at increasing Indo-Pacific **collaboration and exports**.

Asean

Australia currently services all priority ASEAN countries, including Singapore which ranks 4th. **The Federal Government has committed to strengthening economic ties** in ASEAN, which will support further trade.

Japan

Currently **attracts 11 per cent** of exporters. Japan's **rapid digitisation rates** continue to outpace growth in the cyber security sector, presenting an opportunity for international firms to export into the fast-growing market.

Other leading markets: Brazil, Germany, Netherlands, Switzerland, United Arab Emirates, Belgium, France, South Africa, Sweden

Australian demand for cyber security goods and services is forecast to slow to 5.7 per cent by 2024

Growth in Australia's demand for cyber security is expected to slow. Australia's cyber security demand was particularly strong during COVID-19, with growth at 9.1 per cent between 2020 and 2022. By 2024, demand is forecast to slow to 5.7 per cent.

Demand for cyber security was strong during the COVID-19 pandemic due to three reasons:

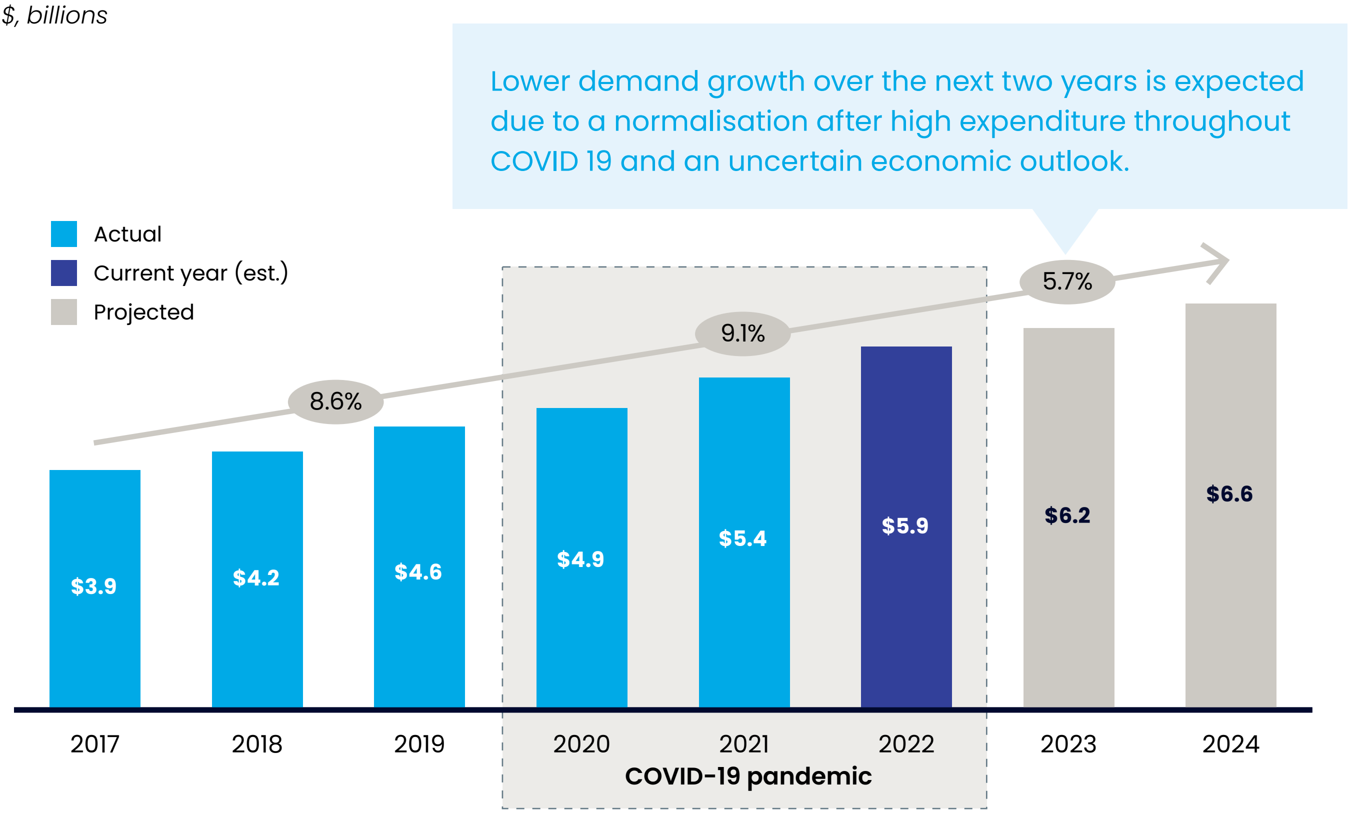
- Accelerated digitisation required accelerated cyber security responses.
- Organisations rapidly implemented remote working solutions for their workforces.
- Scams and cyber attacks increased as a result of the pandemic.

Demand growth in the near term is expected to slow to 5.7 per cent by 2024. A normalisation of organisational cyber security budgets after increased spending during the COVID-19 pandemic and an uncertain economic outlook are expected to slow growth over the next two years. Forecast growth is underpinned by the increased scope of the Security of Critical Infrastructure (SOCI) legislation amended in 2022, growing frequency and severity of attacks, and increased awareness among senior executives and Boards of the risks that insufficient cyber security protections pose.

Estimates of cyber security demand vary. Innate forecasting challenges such as the unpredictability of shocks and economic conditions are exacerbated in the cyber security sector by inconsistent definitions around the scope of the sector and little reporting of the sector in official government statistics.

Australia's cyber security spend, 2017–24[13,14,15]

A$, billions



[13] Gartner Information Security Forecast, Worldwide, 2016–2026, 1Q22 Update
[14] McKinsey (2020)
[15] Expert interviews, Accenture analysis

Australian organisations spend more than half of their cyber security budgets on systems security and software and platform security

Of the categories of cyber security expenditure, Australians spend most on systems security and software and platform security. At $1.6 billion and $1.5 billion respectively, these two product categories account for over 50 per cent of total cyber security spend in 2022.

COVID-19 drove demand for cyber security solutions that supported remote working and protections against opportunistic threats and scams. Within systems security, Australians spend most on managed security service providers (MSSPs) and identity and access management services.[16] MSSPs are critical to monitoring for scams, and identity and access management solutions are critical to supporting remote working.

Australian cyber security firms' offerings mostly reflect Australian demand. Systems security, software and platform security and human, organisational and regulatory services are each offered by more than 35 per cent of Australian firms in 2022. These are also the three areas of cyber security that see the most domestic demand.

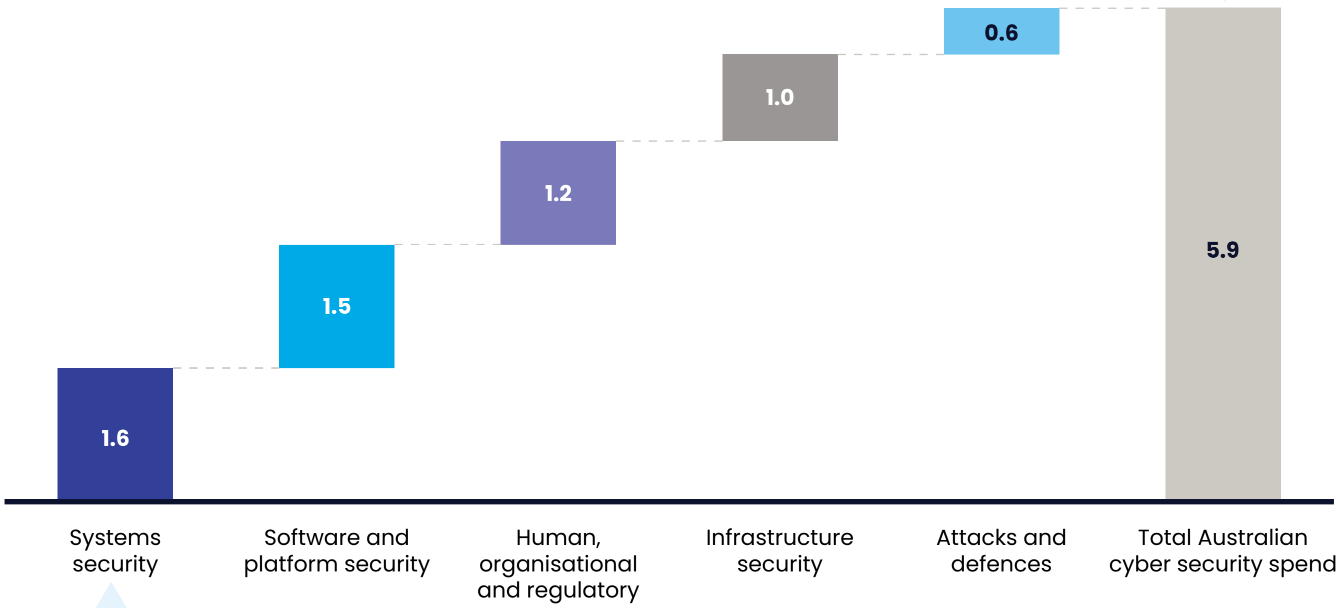
Attacks and defences offerings are sold by 31 per cent of Australian firms, yet it will see the lowest level of spend in 2022. Australian firms offering attacks and defences, and specifically penetration testing are targeting international markets, with 76 per cent of firms who offer attacks and defences solutions exporting penetration testing in 2022. The 2020 SCP found that penetration testing was one of Australia's greatest exports and recommended the Australian sector maintain momentum and focus on this offering.

[16] Gartner Information Security Forecast, Worldwide, 2016–2026, 1Q22 Update

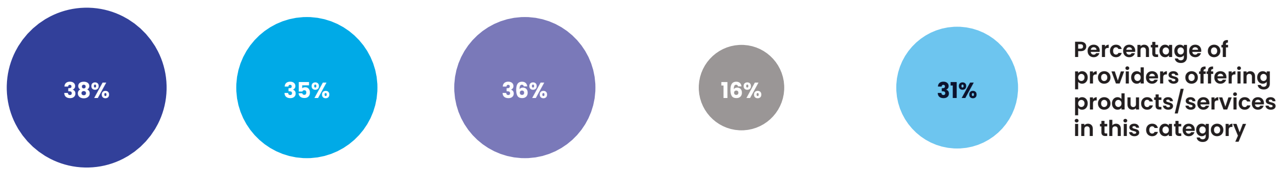
Australia's cyber security spend by product segment, 2022[17,18]

A$, billions

Analysis suggests that a severe cyber attack could cost the economy more up to $12.8 billion – a risk which far outpaces the current national spend on cyber security. Increasing cyber security spend to mitigate against the risk of widespread attacks, similar to the 2022 Optus data breach, could save the economy billions of dollars.



Systems security and software and platform security are the two largest segments and comprise over 50 per cent of total cyber security spend. The composition of expenditure in Australian cyber security has remained largely unchanged since 2020.



[17] AustCyber's Digital Census 2022, "What are the main products and/or services your organisation offers? Of these, which are your top 3 products and/or services?"
[18] McKinsey (2020), Accenture analysis

A normalisation after strong growth due to COVID-19, and an uncertain economic outlook are slowing cyber security sector demand

A downgrading of the cyber security sector's near-term outlook is due to a correction following very strong growth during COVID-19 and an uncertain economic outlook. Both of these factors have very recently impacted the sector, which had experienced very strong growth since 2017.

Cyber security firms performed well during COVID-19 due to strong demand for cyber security products and services. Demand growth in turn drove revenue growth which in turn drove stock prices to increase. From 1 January 2020 to 1 January 2021, some Australian ASX-listed cyber security firms' share prices increased fivefold.

However, performance of cyber security firms has returned to pre-pandemic levels. Demand growth has slowed as organisations reign in their cyber security expenditure following huge outlays during COVID-19. Some industry experts have suggested that many organisations are rationalising their cyber security after haphazard tactical fixes were implemented as workforces moved to remote working. This slowdown has led to stock prices returning to pre-pandemic levels.

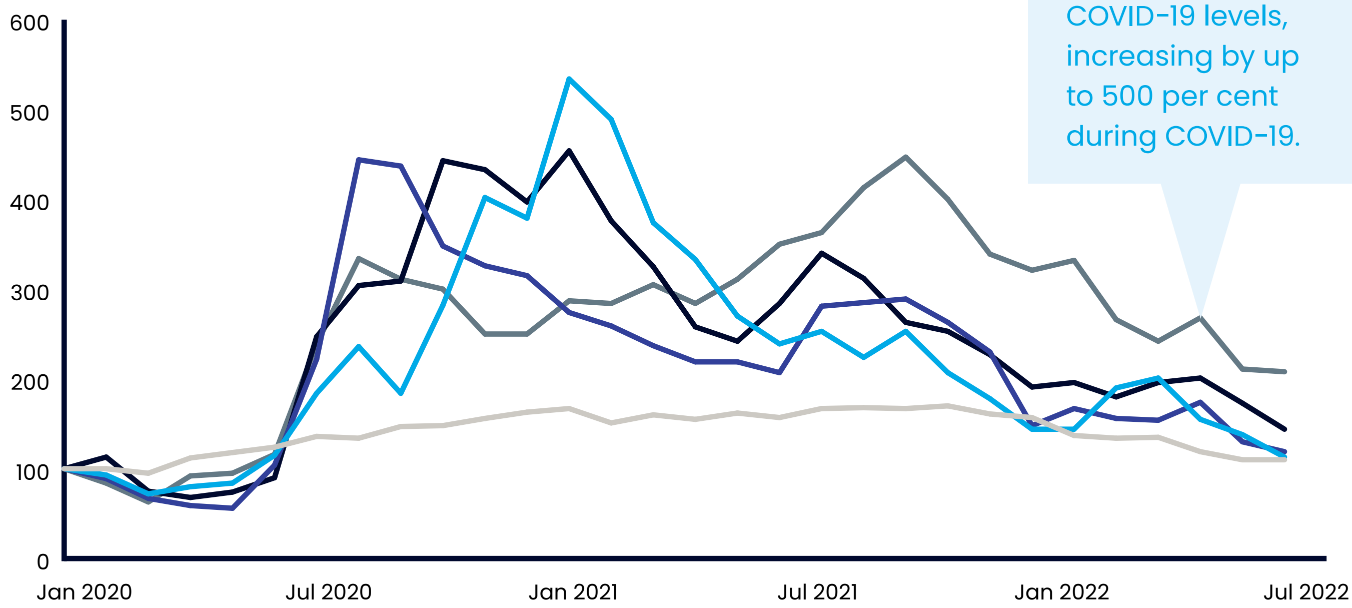
Additionally, Australia faces an uncertain economic outlook which may reduce overall expenditure in the economy. In their May 2022 statement on monetary policy, the RBA forecast economic growth to moderate in 2023 as COVID-19 fiscal policy support is withdrawn and rising prices weigh on real income causing consumption to slow.

Cyber security is expected to be somewhat resilient, but not impervious to economic headwinds. Increasingly, cyber security is viewed as business critical and therefore the sector is not expected to be hit as hard as discretionary goods and services; however, a slowdown in growth seems inevitable.

Australian cyber security firms' share prices have returned to pre-COVID-19 levels, increasing by up to 500 per cent during COVID-19.

Stock value of cyber security firms listed on the ASX[19,20]

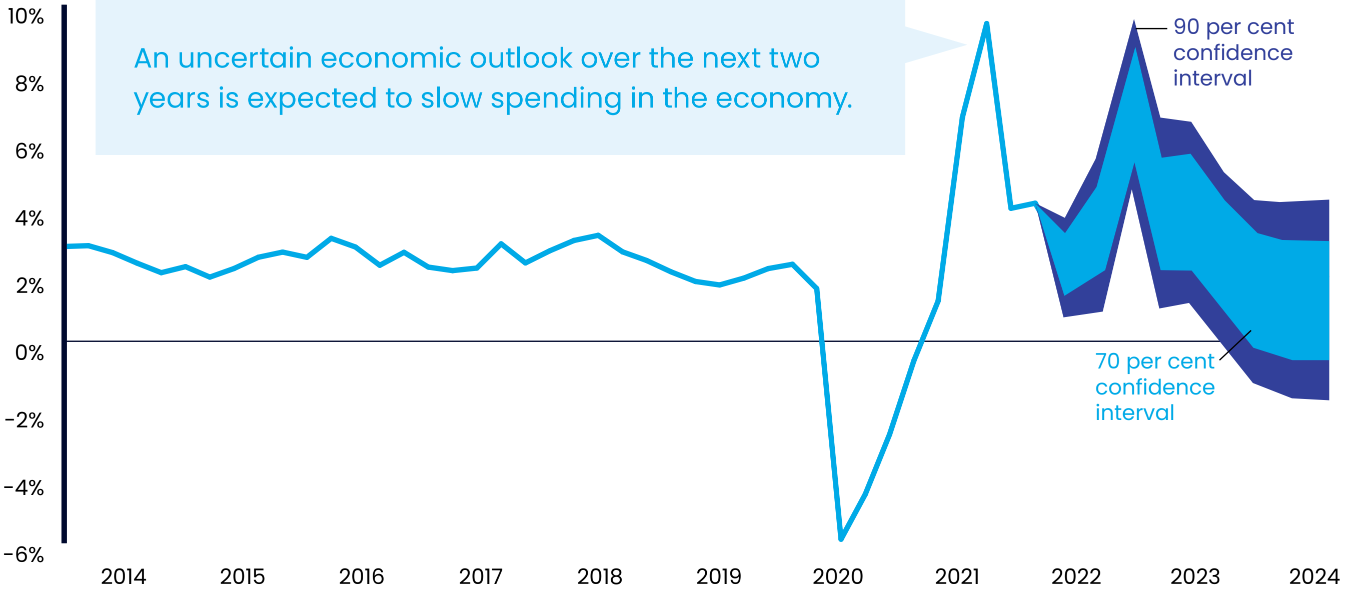
Normalised stock price of select cyber security firms (anonymised) (index = Jan 2020)



Economic outlook[21]

GDP growth forecast (Year-ended)

An uncertain economic outlook over the next two years is expected to slow spending in the economy.



[19] Confidence intervals reflect RBA forecast errors since 1993.
[20] ASX (2022)
[21] RBA (2022)

Domestic demand for cyber security will be shaped by new technologies and external pressures

While growth is expected to slow in the near term, demand for cyber security is still increasing, and the sector needs to be prepared for new technologies and an emerging threat environment.

Cloud computing is expected to drive demand in the cyber security sector in the next three years. While demand growth is expected to slow in the near term, more data being stored in the cloud drives the need for cyber security solutions. Uptake of cloud data storage solutions is higher in Australia than almost anywhere else in the world. Larger organisations in Australia are more mature than smaller firms in their use of the cloud, but SMEs are following suit.

A changing geopolitical outlook is also expected to impact the sector. Tensions around the world are expected to increase the frequency and severity of attacks. Additionally, increased geopolitical risks are driving demand for a sovereign cyber security capability. Cyber security firms surveyed in AustCyber's Digital Census 2022 agreed that the leading cyber security threat actors in Australia will shift from financially motivated cyber criminals to geopolitically motivated nation states within the next five years.

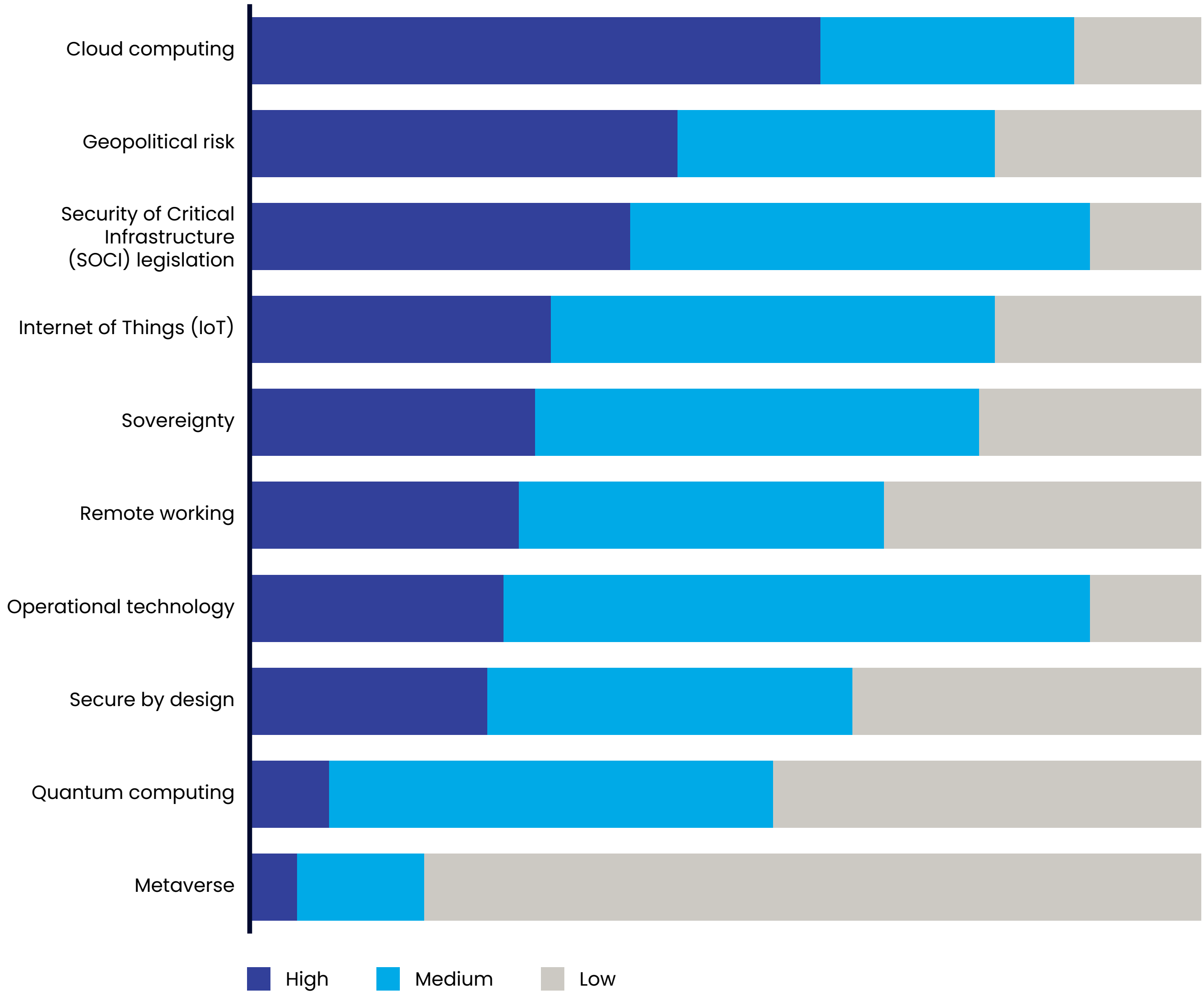
Security of Critical Infrastructure (SOCI) legislation mandates cyber security protections for 11 critical sectors. The Act mandates additional cyber security protections, which is driving domestic demand for cyber security. The SOCI legislation captures 11 critical sectors: energy, food and grocery, healthcare and medical, data storage and processing, transport, water and sewerage, defence, higher education and research, space technology, communications, financial services and markets.

Emerging technologies such as quantum computing could have profound impacts on the sector. Quantum computers are expected to be able to decode current cryptography, which would compromise most existing cyber security protections.[20]

22. American Scientist (2019), expert interviews

Top trends impacting cyber security over the next three years[23]

Share of survey responses



[23] AustCyber's Digital Census 2022 "In the next 3 years, to what extent will the following trends impact on the cyber security industry in Australia? ", Accenture analysis

Cyber security degree enrolments and course offerings have increased since 2014, with over 8,000 higher education enrolments in 2020

Cyber security-specific VET and university enrolments increased to 8,200 in 2020. Of these, 5,000 students were enrolled in VET and 3,200 students were enrolled at universities. More than 90 per cent of VET students took up Certificate IV training, with the remainder undertaking a diploma or advanced diploma. University enrolments include undergraduate or postgraduate degrees.

While the growth in enrolments has been fast, maintaining this momentum will be vital. To meet the sector's need of 3,000 additional workers by 2026, enrolments in cyber security courses will be vital to ensure Australia's workforce keeps pace with projected growth. Enrolments need to increase to 2026, taking into account that not all enrolled students will finish up working in Australia's cyber security sector, due to course incompletions, international migration (particularly from the international student cohort) and students finding employment in other sectors.

Cyber security offerings in the university and VET systems have continued to increase since 2020. More than 20 universities now offer cyber security as a specialist degree or as a major in information technology or computer science degrees. During COVID-19, additional new course offerings have been made available to provide flexible training to a wider audience. For example, AustCyber and TAFE NSW launched a program of short courses to help workers retrain and upskill into cyber security. Additionally, CSIRO has begun offering free cyber security training for small and medium-sized businesses.

Course offerings

First cyber security programs (2011–2014)

Australia ECU Edith Cowan University

Curtin University

Early support (2014–2017)

La Trobe University

Macquarie University

Charles Sturt University

UNSW Sydney

Box Hill Institute

Canberra Institute of Technology CIT

University of South Australia

Institutions mobilising (2018–2019)

NSW Government TAFE NSW

Western Sydney University

tafeSA

The University of Adelaide

Deakin University Australia

tafe Queensland

Continued growth (2020+)

RMIT University

CSIRO

Griffith University

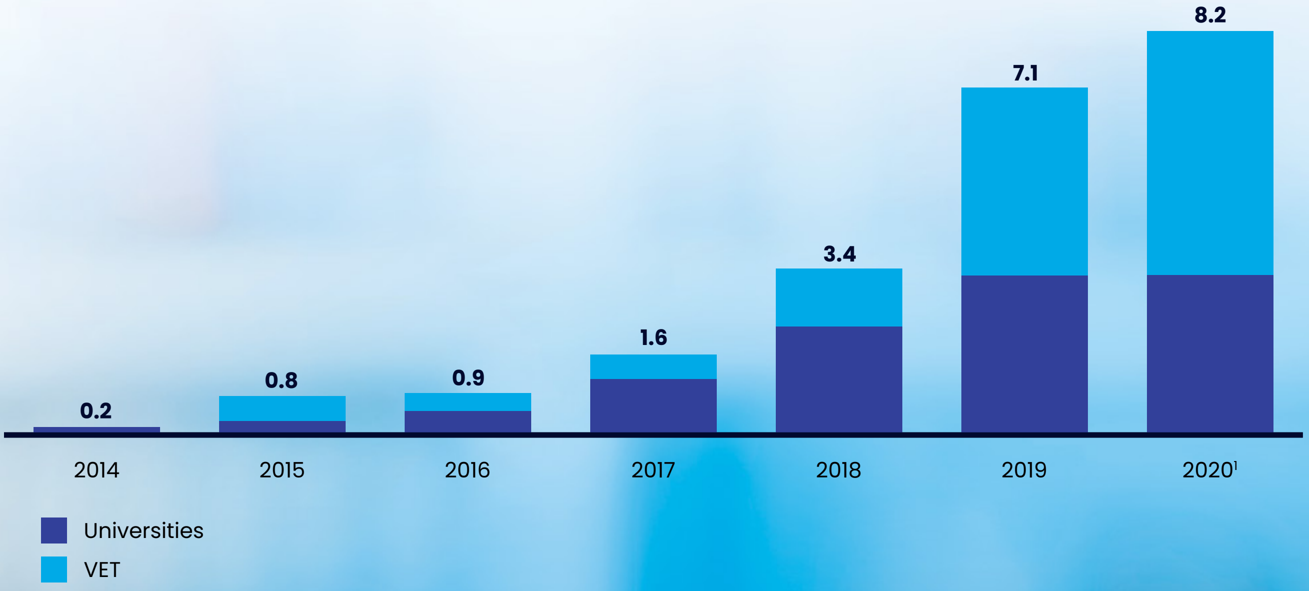
NSW Government TAFE NSW

AustCyber

Western Australia Innovation Hub

Cyber security-specific VET and university courses and enrolments[24,25,26,27,28]

Number of students ('000) between 2014–20



[24] See Appendix C for detailed methodology

[25] Enrolment data for 2020 is the most recent data available.

[26] NCVER DataBuilder (2022)

[27] DESE (2022)

[28] Prosple (2021), Accenture analysis

Representation of women in cyber security is slightly lower than representation in the broader ICT sector, which is at 31 per cent

Females represent only 26 per cent of the Australian cyber security workforce in 2022. Australia's cyber security sector falls five percentage points behind the broader ICT sector on females in the workforce, which is at 31 per cent.

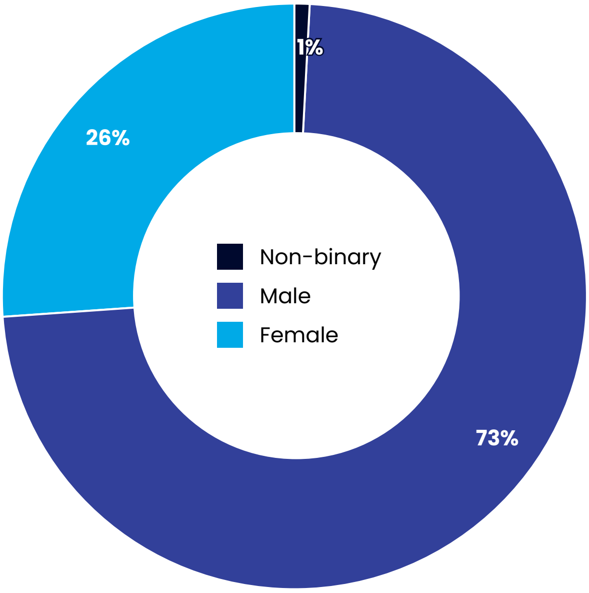
Globally, females account for 24 per cent of the cyber security workforce, up from 11 per cent in 2013. While slightly better than the global average, Australia is outperformed by some regions including Southeast Asia where female representation in cyber security is 30 per cent.[29]

Whilst progress has been made in promoting gender diversity in cyber security, there is still more to be done. Survey respondents suggest that the gender imbalance still poses a problem for the sector and that early progress indicates the benefit that embracing gender diversity in cyber security could bring. Respondents also recognise potential action to improve gender diversity, including encouraging girls to take up STEM and increasing support and sponsorship of women in cyber security roles.

The domestic cyber security sector can benefit from diversity and inclusion in the workforce. Industry experts suggest that greater diversity in the cyber security talent pool will help ease the pressure of the national skills shortage, as well as boost innovation in the sector due to input from more diverse backgrounds.

Cyber security workforce by gender 2022[30]

Percentage of survey respondents



- Females account for 26 per cent of the cyber workforce in Australia, **consistent with international female representation** in cyber security at ~24 per cent.[30,31]
- Representation of women in cyber security is slightly **higher than representation in the broader ICT sector,** at 31 per cent.[32]
- Despite fewer years' experience, **women earn more cyber security certifications than males** on average. Similarly, 52 per cent of women hold a postgraduate degree, compared with 44 per cent of men.[30,31]

[29] (ISC)2 (2021)
[30] AustCyber's Digital Census 2022 – "At the end of the 2021/22 financial year, what do you expect the demographic makeup of your workforce to be? Please describe how AustCyber can assist the sector to boost women's participation in the cyber security workforce?"
[31] (ISC)2 (2021)
[32] ACS (2022), Accenture analysis

Improving gender diversity in cyber security

Select survey responses when asked how AustCyber can support women's participation in cyber security

"Female representation is a significant problem for our industry that needs to be improved."

"The momentum today is improving across many fields. We can ride the wave and learn from successes in other industries."

"There are many great initiatives currently to support women and diverse groups in security."

"We're seeing some wonderful female operators come through and I'm proud to employ a number of them. Let them cultivate, grow and become awesome individuals."

New South Wales is home to the majority of cyber security firms in the country

Overview

NSW is home to the largest number of cyber security firms in the country, with the state's 87 firms accounting for 30 per cent of the total sector.[33] NSW has a mix of well-established firms (many more than 20 years old) and young firms. 34 per cent of firms in NSW are less than five years old, including notable new firms such as Peakhour, Sekuro and TriSecOps.

Key industries and customers

Cyber security firms in NSW service all industries but primarily serve financial services, government and IMT clients. The largest cyber security customer groups in NSW are SMEs and large organisations. The greatest demand from NSW cyber security customers comes from systems security and software and platform security offerings, which is in line with national demand.

Cyber security node priority areas

The NSW Cyber Security Innovation Node was established through a bilateral partnership between AustCyber and the NSW Government. The node is focusing on cyber security applications in Industry 4.0, financial services, digitisation and cyber security workforce development.

Exporting

According to the findings from AustCyber's Digital Census 2022, 58 per cent of cyber security firms based in NSW export. Firms in NSW most commonly export to the US, UK, the Philippines and Brazil.[34]

Workforce

79 per cent of the NSW workforce is located in Sydney, Wollongong and Newcastle. The remaining 21 per cent of the workforce is located in regional areas. The NSW cyber security workforce is 28 per cent female; slightly higher than the national average of 26 per cent. The NSW government body responsible for cyber security, Cyber Security NSW, is leading the way with regards to gender parity, achieving a 50 per cent female workforce in 2021.[35] NSW has an opportunity to continue the momentum on gender diversity as the sector grows.

State Government support

The government announced in the 2022–23 NSW Budget that it will release an additional $126.7 million from the $2.1 billion Digital Restart Fund from 2022 to 2025. $37.9 million of this will be allocated to uplifting the state's cyber security threat management and systems.

New South Wales overview

87 cyber security firms are headquartered in NSW

Median age of cyber security firms is **5.5** years

34% of firms in NSW are less than five years old

58% of cyber security firms are exporting

Cyber security node priority areas:

1. Industry 4.0
2. Digitisation
3. Cyber security workforce development
4. Financial services

Cyber security educational institutions:

Western Sydney University

NSW Government TAFE NSW

The University of Newcastle Australia

The University of Sydney

Macquarie University

Charles Sturt University

UTS University of Technology Sydney

UNSW Sydney

[33] Firm count is based on firms registered with AUCYBERSCAPE. The total number of firms is likely to be larger than is illustrated here.
[34] AustCyber's Digital Census 2022, Crunchbase (2022)
[35] Digital NSW (2021), Accenture analysis

Victoria is Australia's second largest market and has a strong base of exporting firms

Overview

Victoria is home to 67 cyber security firms making up 23 per cent of the total Australian cyber security sector.[36] The median firm age in the state is five years, on par with the national average. Less that half of Victorian firms are less than five years old, including new entrants such as ARGOS, Cydalics and DroneSec. Like NSW, Victoria also has a strong presence of mature firms over 20 years old.

Key industries and customers

Cyber security firms in Victoria predominantly serve clients in financial services, government, professional services and consulting, and IMT. As well as SMEs and large organisations, Victorian cyber security firms serve local, state and federal governments. Victoria's cyber security firms primarily offer software and platform security and systems security, with operating systems and virtualisation security being the leading offerings in Victoria.

Exporting

Consistent with a mature market, half of Victoria's cyber security firms export overseas. According to the AustCyber's Digital Census 2022, 52 per cent of Victorian firms export, compared to 46 per cent in 2020. The most common export markets for Victorian cyber security firms are the US, UK, New Zealand, Canada, Poland and Singapore.[37]

Workforce

Relative to other states and territories, Victoria's workforce is highly concentrated in the capital, with 85 per cent based in Melbourne. The workforce is 22 per cent female, lower than the national average of 26 per cent. Female representation in the Victorian cyber security sector is also well below its broader digital technology sector, at 31 per cent.[38] However, in May 2022, the Victorian government launched the $100,000 Women in Security Pilot Program to boost the number of women employed in the state's cyber security sector. The program is targeted at women currently working in the tech sector who are interested in increasing their cyber security knowledge in order to move into leadership positions.

State government support

The government released Victoria's Cyber Strategy 2021 and set out to offer funding of $50.8 million over the next five years. The strategy outlines the missions of safe and reliable delivery of government services, a cyber safe environment for the community and a vibrant cyber security economy.[39,40]

Victoria overview

67 cyber security firms are headquartered in VIC

Median age of cyber security firms is **5** years

47% of firms in VIC are less than five years old

52% of cyber security firms are exporting

Cyber security node priority areas:

- Victoria are in the process of establishing an innovation node as well as cyber security node priority areas.

Cyber security educational institutions:

Federation University Australia
Deakin University Australia
Victoria University
The University of Melbourne
La Trobe University
Chisholm
Melbourne Polytechnic
Swinburne University of Technology
holmesglen
RMIT University
Monash University
Box Hill Institute

[36] Firm count is based on firms registered with AustCyber. The total number of firms is likely to be larger than is illustrated here.
[37] AustCyber's Digital Census 2022
[38] Victoria State Government Jobs, Precincts and Regions (2022)
[39] Victoria State Government Cyber Security Strategy (2021)
[40] Victoria State Government Budget (2021), Accenture analysis

Queensland has one of Australia's most mature cyber security markets

Overview

Queensland is home to 49 cyber security firms, which account for almost 17 per cent of the nation's cyber security firms.[41] The state has a more mature cyber security industry, with a median firm age of seven years. However, 35 per cent of the firms in Queensland are under five years old, such as Akela Digital, Suncoast Information Security and Process Landscape.

Key industries and customers

Cyber security firms in Queensland predominantly serve clients in resources, IMT, financial services and government. Queensland cyber security firms' customers span all levels of government, SMEs and individuals. The most frequently purchased cyber security offerings by firms in Queensland are human, organisational and regulatory offerings.

Cyber security node priority areas

Three Cyber Security Innovation nodes have been established in Queensland since June 2020; in Brisbane, Townsville and the Sunshine Coast. The nodes will help strengthen Queensland's position in the Australian cyber security sector, particularly in the priority areas of defence and the supply chain, advanced manufacturing, health, education and agritech sectors.

Exporting

47 per cent of Queensland's cyber security firms export, according to the results from AustCyber's Digital Census 2022. New Zealand, the Netherlands, Singapore, the US, United Arab Emirates and the UK are Queensland's most popular export markets.[42]

Workforce

Queensland has a lower proportion of women in its cyber security workforce than other states and territories. The Queensland cyber security workforce is 14 per cent female, in comparison to 26 per cent nationally. Queensland is the only state or territory where the majority of the workforce is located outside of the capital, with only 34 per cent of the workforce based in Brisbane.

State government support

The government announced in the 2021–22 Queensland budget that it will release an additional $11 million over two years for government cyber security enhancements. In addition, the state launched two new Cyber Security Innovation Nodes in Brisbane and Townsville during 2021.[43,44]

Queensland overview

49 cyber security firms are headquartered in QLD

Median age of cyber security firms is **7** years

35% of firms in QLD are less than five years old

47% of cyber security firms are exporting

Cyber security node priority areas:

1. Defence and the supply chain
2. Advanced manufacturing
3. Health
4. Education
5. Agritech

Cyber security educational institutions:

QUT

Griffith UNIVERSITY

UNIVERSITY OF SOUTHERN QUEENSLAND

tafe Queensland

USC AUSTRALIA

THE UNIVERSITY OF QUEENSLAND AUSTRALIA

[41] Firm count is based on firms registered with AustCyber. The total number of firms is likely to be larger than is illustrated here.
[42] AustCyber's Digital Census 2022, Department of Tourism
[43] Innovation and Sport (2021)
[44] Queensland Government (2021), Accenture analysis

The ACT cyber security sector specialises in providing services to Australian Government and defence clients

Overview

The Australian Capital Territory (ACT) is home to 42 cyber security firms, accounting for 15 per cent of Australia's cyber security sector.[45] The median age of firms in the ACT is five years old. One quarter of the firms in the ACT are less than five years old, including Syconic Cyber and Cobalt.

Key industries and customers

Cyber security firms in the ACT primarily provide products and services for governments, both the Commonwealth Government and a number of international governments. Customers of these cyber security firms primarily purchase offerings related to software and platform security, and attacks and defences.

Cyber security node priority areas

The Canberra Cyber Security Innovation Node was established in 2017, through a partnership between the ACT Government and AustCyber. The Insurance Australia Group Limited (IAG) is responsible for promoting the Canberra cyber security sector, providing strategic direction to the Canberra node and overseeing the implementation of its work plan. The node is growing and creating jobs while strengthening Canberra's knowledge economy, particularly in the priority areas of space, defence, and education sectors.

Exporting

The results from AustCyber's Digital Census 2022 suggest that 56 per cent of firms based in the ACT are exporting. The US and UK are the top international markets in 2022 by number of firms exporting.[46]

Workforce

Gender diversity in the ACT's cyber security workforce is on par with the national cyber security workforce, at 26 per cent female representation.

Government support

Between 2021 and 2025, the ACT Government will spend $10.3 million on a cyber security centre to improve cyber security resilience and to protect the ACT Government's ICT network. The ACT Government will also support Canberra Cyber Hub through an initial investment of $700,000. The funding will go towards accelerating the growth of SMEs, offering students and businesses more education opportunities and promoting cyber security capabilities in Canberra.[47]

Australian Capital Territory overview

42 cyber security firms are headquartered in the ACT

Median age of cyber security firms is **5** years

38% of firms in the ACT are less than five years old

56% of cyber security firms are exporting

Cyber security node priority areas:

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

Cyber security educational institutions:

UNSW Sydney

Canberra Institute of Technology

University of Canberra

Australian National University

[45] Firm count is based on firms registered with AustCyber. The total number of firms is likely to be larger than is illustrated here.
[46] AustCyber's Digital Census 2022
[47] ACT Government 2021–22 Budget (2021), Accenture analysis

The Western Australian cyber security sector is focused on resources, logistics, defence and technology

Overview

Western Australia (WA) is home to six per cent of the nation's cyber security firms, with 20 firms having their headquarters in the state.[48] WA's cyber security sector is the youngest of any state or territory. The median age of firms in WA is five years, with one in four firms establishing within the last five years. Some of the most recent firms to establish in WA include Tannhauser, Yira Yarkiny and Retrospect Labs.

Key industries and customers

Cyber security firms in WA primarily serve large organisations in energy and utilities, and governments. A focus of cyber security firms on energy and utilities is unique to WA and consistent with their economy. WA firms procure 20 per cent of the nation's total cyber security revenue, and 13 per cent of the state's firms service these clients. 19 per cent of WA cyber security firms have flagged defence as a target customer group in 2022. However, only four per cent of WA firms currently service defence clients. The cyber security solutions sold most frequently by WA firms fall into the categories of systems security and software and platform security, which is consistent with national figures.

Cyber security node priority areas

The three priority areas of the WA Node are critical infrastructure, cybercrime and big data. The node engages with multiple sectors in WA including mining, oil and gas, agriculture, freight and logistics, defence and technology transfer opportunities with digitally focused small and medium-sized enterprises.[49]

Exporting

According to the latest available data, 44 per cent of firms in WA are exporting.

Workforce

The WA cyber security workforce consists of 25 per cent women, which is consistent with the national average of 26 per cent. 88 per cent of WA's workforce is based in Perth, which is high compared to other states and territories. This is consistent with a young sector and with the cyber security node being located within the capital. The distribution of the sector is expected to spread further into other regions as the WA cyber security sector matures.

State government support

The WA Government allocated $25.5 million from the Digital Capability Fund to enhance the state's cyber security services, which will allow for additional cyber security services across the public sector and increase the Office of Digital Government's Cyber Security Unit.[50]

Western Australia overview

20 cyber security firms are headquartered in WA

Median age of cyber security firms is **5** years

25% of firms in WA are less than five years old

44% of cyber security firms are exporting

Cyber security node priority areas:

1. Critical infrastructure
2. Cybercrime
3. Big data

Cyber security educational institutions:

Australia ECU University Edith Cowan

Curtin University

TAFE International Western Australia

Murdoch University Perth | Singapore | Dubai

[48] Firm count is based on firms registered with AustCyber. The total number of firms is likely to be larger than is illustrated here.
[49] AustCyber's Digital Census 2022
[50] Western Australia Government (2022), Accenture analysis

South Australia's mature cyber security market serves primarily government, business and individual clients

Overview

South Australia (SA) has 23 firms with primary headquarters in the state, representing eight per cent of the cyber security firms in the country.[51] The cyber security firms in SA are older than the firms in most other states and territories, as the median age of firms in the state is nine years. Despite the high median age of firms in SA, 29 per cent of the state's cyber security firms are under five years old. StarkNEX is an example of a new entrant in SA.

Key industries and customers

Cyber security firms in SA have clients from a wide variety of industries, including manufacturing, construction, financial services, professional services and consulting, and defence. Cyber security firms in SA mainly provide systems security and software and platform security offerings, which is in line with broader national provision. The customers of SA cyber security firms are diverse, including domestic and international governments, SMEs, large businesses and individuals.

Cyber security node priority areas

The South Australia Node works closely with government, industry and academic and research institutions in South Australia. The node is growing and showcasing skills in cyber security, while strengthening collaboration between SA's private, public and academic sectors, particularly in the priority areas of space, defence and the supply chain, autonomous systems, digital health and education sectors.

Exporting

29 per cent of cyber security firms in SA report that they are exporting in 2022. South Australian exporters are selling to 23 countries, spanning North America, Europe, Asia, the Middle East, the Pacific and Africa.[52]

Workforce

SA has a lower percentage of women in its cyber security workforce than other regions, with just 15 per cent, compared to the national workforce of 23 per cent. South Australia has the highest workforce concentration in the capital city, with 90 per cent of the workforce based in Adelaide.

State government support

The SA Government has announced a Hi-Tech Sector Plan 2030, which outlines cyber security priorities for the state. As part of SA's broader commitment to enhancing the cyber security sector, the state has invested in an $8.9 million Australia Cyber Collaboration Centre, which is based in the Lot Fourteen precinct. The SA Government is also committed to improving the state's cyber security resilience to threats, with $20.6 million of funding allocated in the State Budget 2021–22 for this purpose.[53]

South Australia overview

23 cyber security firms are headquartered in SA

Median age of cyber security firms is **9** years

29% of firms in SA are less than five years old

29% of cyber security firms are exporting

Cyber security node priority areas:

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

Cyber security educational institutions:

University of South Australia

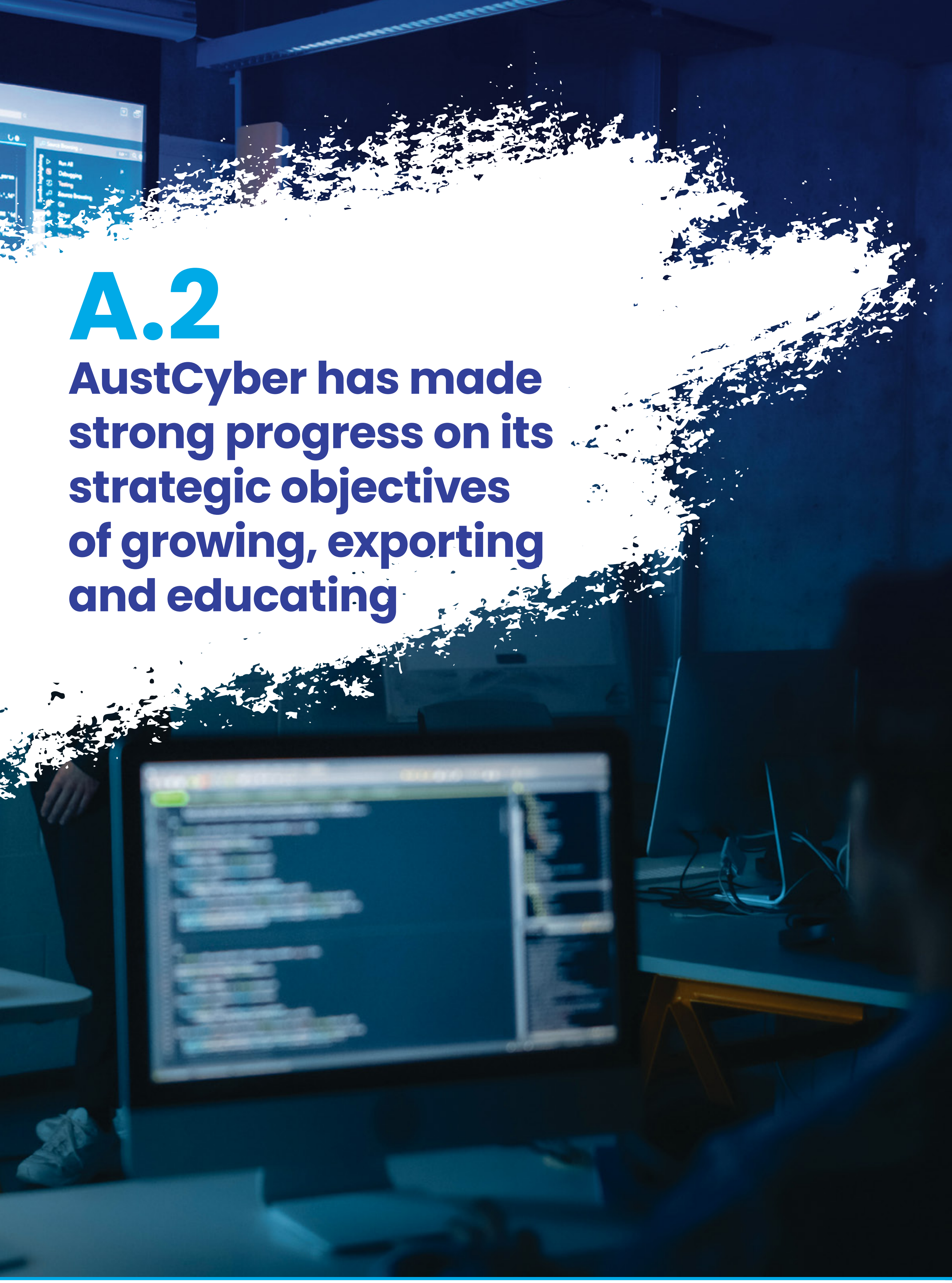
THE UNIVERSITY of ADELAIDE

tafeSA

Flinders UNIVERSITY

TORRENS UNIVERSITY AUSTRALIA

[51] Firm count is based on firms registered with AustCyber. The total number of firms is likely to be larger than is illustrated here.
[52] AustCyber's Digital Census 2022
[53] South Australia Government (2020), Accenture analysis



A.2

AustCyber has made strong progress on its strategic objectives of growing, exporting and educating

AustCyber has supported growth projects to enable the development of the sector, including Penten's mobility program

1 Grow

Grow an Australian cyber security ecosystem

Penten has received over $2.3 million in funding through AustCyber, which enables it to create a product that has revolutionised defence procurement.[1,2]

Summary

Founded in 2014, Penten is an Australian-owned, multi-award winning cyber technology firm that offers unique, sovereign capability to deliver new defence and security technologies for the future fight.

Penten's advanced hardware and software products and services support government and defence clients with secure mobility, applied AI and tactical communications security solutions.

Penten aims to deliver world-leading security technologies to realise digital advantages for the nation and to enable the modern warfighter and policymaker with information to deliver these advantages.

"SMEs are the future growth and innovation engine of the Australian cyber security economy. These businesses provide invaluable opportunities for Defence to gain advantage. Without them, we are missing out. Australia is missing out."

- Matthew Wilson, CEO, Penten

Impact

Penten's mobility program, launched in 2020, **provided fly away kits to a pilot group of regional SMEs and academia**, enabling them to access their own classified IT network on a scalable, multi-tenant service.

SenseNet as a Service (SNaaS) aims to provide sector and academia **secure access to sensitive or classified information** so they can work with defence and government clients.

The launch of this project represented a turning point for the defence industry. The opportunity will provide Australian SMEs with the means **to bid for, win and work on Government classified projects** in a secure and protected environment from any location. Regional Australia will no longer be excluded from working on Defence projects and Australia's sovereign defence capabilities will have a chance to thrive.

[1] AustCyber (2022)
[2] Penten (2020), Accenture analysis

Investment and support from AustCyber has allowed Australian firms like HackHunter to access opportunities in export markets

HackHunter®

2 Export

Export Australian cyber security to the world

With $268,000 in funding from AustCyber, HackHunter developed a WiFi tracker product, which is now being sold around the globe.[3,4]

Summary

HackHunter is an Australian cyber security IoT provider based in Melbourne.

Established in 2018, HackHunter offers a suite of two wireless communication protection products – the Pursuit portable WiFi tracker and the Vision continuous monitoring sensor.

HackHunter's security products allow users to detect unauthorised WiFi, alert if it is malicious and locate the source with precision, all in real time.

> *"The new concept of cyber security has implications beyond Australia, with a large proportion of our value chains dependent on the digital security of other countries."*
>
> **- Michael Bromley, CEO, AustCyber**

Impact

HackHunter launched the Pursuit portable WiFi tracker in November 2020, remarkably, only eight months after the development of the initial prototype. At the end of the project, HackHunter had a **market-ready product** which had been trialled in Australia, Canada, the US, Malaysia and the EU. It was purchased by the Australian Government Department of Defence and by insurance companies in Australia and Canada.

HackHunter has **ongoing negotiations for direct sales** to customers overseas and, through partnerships, to law enforcement, government, defence, telecommunications and finance industries in Australia, Asia and the EU. HackHunter's technologies are designed, developed and manufactured in Australia. HackHunter won the Australian Information Security Association (AISA) **2020 Award for Cyber Security Start Up of the Year.**

[3] AustCyber (2022)
[4] HackHunter (2022), Accenture analysis

AustCyber has actively supported cyber security education through funding and assistance for programs such as Untapped's Genius Armoury

untapped.

3 Educate

Make Australia the leading centre for cyber education

$160,000 in funding from AustCyber enabled Untapped to launch its cyber security education program designed to support neurodiverse talent.[5,6]

Summary

Untapped is an Australian organisation based in Melbourne with an extremely wide range of activities supporting employment of neurodiverse talent, from pathways to employment to ongoing development once employed.

Untapped leads and funds a range of initiatives globally, including the internationally recognised Neurodiversity Hub, Australian Autism@Work Summit, consulting to universities and employers, delivering government-funded projects to improve outcomes for autistic young adults, funding and deploying research relevant to neurodiverse employment programs and sponsoring the development of life skills training for neurodiverse individuals by a neurodiverse team.

Impact

In 2021, Untapped Holdings launched a new platform, **Genius Armoury**, to provide foundation-level **cyber security training** and career pathways information to the **neurodiverse community**. The platform is an online environment designed to identify and attract a previously untapped cyber security talent pool from within the autistic community.

Genius Armoury comprises five modules:

1. Introduction to cyber security
2. Threats and exploits
3. Networks
4. Digital forensics
5. Cyber security tools
6. Governance, risk and compliance

As much as the platform was designed to enable neurodivergent individuals to commence education and a career in cyber security, it has also inspired neurotypical workers who had not previously considered a cyber security career.

The benefit to Australia is an overall **expansion of the potential talent pool** that organisations can invest in to meet their future cyber security skills shortages.

[5] AustCyber (2022)
[6] Untapped (2022), Accenture analysis

A.3
Cyber security taxonomy

Cyber security product categories

As digital technology evolves, so does cyber security. To a layperson, cyber security might mean firewalls and off-the-shelf antivirus software, but that understanding 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, like much of digital technology, 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 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 from intruders, 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 security 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, through 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 industries to study the sector.

Cyber security product categories

Segment of the cyber security sector	Examples
Infrastructure security	• Managed security service provider • Security operations centres • Security hardware and physical systems
Systems 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 security 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 security-related professional services

2021 update to cyber security ANZSCO codes

Current and new six-digit ANZSCO breakdown of cyber security roles

1	**135111** Chief Information Officer	**135111** Chief Information Officer Chief Information Security Officer Specialisation **[NEW]**
2	**135112** ICT Project Manager	**135112** ICT Project Manager ICT Security Project Manager Specialisation **[NEW]**
3	**261312** Developer Programmer	**261312** Developer Programmer Cyber Security Developer Specialisation **[NEW]**
4	**261313** Software and Applications Programmers	**261313** Software and Applications Programmers Cyber Security included in Description/Lead Statement **[NEW]**
5	**261313** Software Engineer	**261313** Software Engineer **261315** Cyber Security Engineer **261316** Devops Engineer
6	**261314** Software Tester	**261314** Software Tester (a) **261317** Penetration Tester
7	**262112** ICT Security Specialist	**262114** Cyber Governance Risk and Compliance Specialist **262115** Cyber Security Advice and Assessment Specialist **262116** Cyber Security Analyst **262117** Cyber Security Architect **262118** Cyber Security Operations Coordinator

Greater granularity in ANZSCO will improve...

1

Role recognition

Greater recognition of a broader set of specialised cyber security roles

2

Skills recognition and management

Enables skills to be identified and standarised across roles, allowing skills gaps to be better identified and rectified

3

Education standardisation

Creates a benchmark for the development of curricula and course content

4

Workforce strategy

Firms can use the framework to improve the maturity of their hiring and workforce development practices

A.4
Value at risk

The cost of a cyber attack depends on the type of attack, the target and the time it takes to detect and to resolve

1. Type of cyber attack	2. Target	3. Time to detect	4. Time to resolve
• The costs of a cyber attack are dependent on the **type of cyber attack or scenario.**	• The costs of a cyber attack are dependent on the **targeted organisation.**	• If a **cyber attack takes longer to detect,** the costs are likely to be increased.	• Regardless of when the attack is detected, if a **cyber attack takes longer to resolve,** the costs are likely to be increased.
Examples from least costly to most costly:	**Examples from least costly to most costly:**	**Examples from least costly to most costly:**	**Examples from least costly to most costly:**
• scanning or reconnaissance • low-level malicious attack • active network intrusion • exfiltration or deletion/damage of key sensitive data • sustained disruption of essential systems.	• members of the public • small organisations • medium-sized organisations • state government, large organisations • federal government, national infrastructure • national security.	• If an attack is detected quickly the costs are usually minimised as the implications of the attack are reduced. • Attacks that go undetected for weeks or months have higher costs associated with them as the opportunity to do damage is greater.	• If an attack is resolved quickly the costs are typically minimised as the implications of the attack are reduced. • If it is not possible to resolve the attack quickly, the costs will mostly continue to grow until remediation has occurred.

These four factors contribute to the costs of a cyber attack:

Total cost of a cyber attack =	**Cost of attack type**	**+ Cost associated with target**	**+ Time taken to detect**	**+ Time taken to resolve**

Cyber attacks lead to four categories of impact: direct costs, business losses, flow-on effects and intangible costs

Types of costs and effects associated with a cyber attack[3]

Type of costs (not exhaustive)

1. Direct costs	Example
Ransoms	• **Demanded ransoms,** e.g. to gain access to systems during a ransomware attack.
Cyber security	• **Cyber security products**, e.g. firewall and two-factor authentication. • **Cyber security services,** e.g. penetration testing and auditing.
Supply chain security	• **Cyber security for the supply chain,** e.g. risk management for firms in the supply chain.

2. Business losses	Example
Wages and salaries	• **Wages that need to be covered** during a cyber attack, e.g. salaried staff that cannot work.
Lost revenues	• **Lost revenues** due to inability to work during a cyber attack, e.g. due to a loss of sales.
Resource allocations	• **Resource allocations** to resolve the cyber attack, e.g. to restore data and files after a destructive cyber attack.

Business losses are generally the **biggest costs of cyber attacks.**

Cyber security attack

3. Flow-on effects	Example
Supply chain costs	• **Reduced spending in the supply chain,** due to lost revenue, e.g. lower spending in inputs for products.

4. Intangible costs	Example
Deterrent to digitalisation	• **Cyber attacks could deter businesses from digitisation,** e.g. cyber security concerns from SMEs.
Reputational damage	• **Reputational damage from a cyber attack,** e.g. loss of trust or confidence with customers.

1. CISA (2020)
2. Forbes (2022), Accenture analysis
3. Accenture analysis
4. AustCyber's Digital Census 2022 – "How would you rate the cyber security maturity of Australian firms in the below customer groups?"

A lack of cyber security maturity means small and medium businesses are most vulnerable to attacks

Cyber security experts suggest that small and medium businesses are most vulnerable to cyber attacks. 68 per cent of experts surveyed in AustCyber's Digital Census 2022 thought that small and medium businesses had only a 'basic' level of cyber security hygiene. This is supported by a 2021 report which found that over 60 per cent of small and medium businesses spent less than $1,000 on cyber security annually.[5,6]

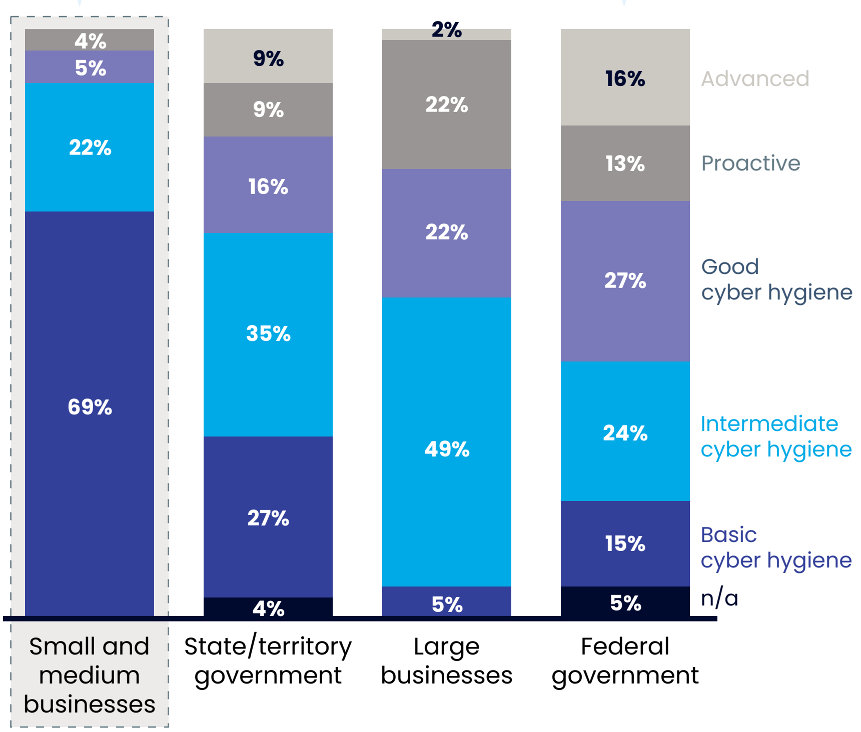
Cyber security experts suggest that large businesses have relatively higher levels of cyber security. Most industry experts (95 per cent) think that large businesses have at least intermediate cyber security hygiene. Large firms devote a greater proportion of resources to information technology and cyber security. Increasingly, large firms also have more mature cyber security capabilities.[7]

Cyber security maturity of Australian organisations

Experts' ratings of cyber security maturity (percentage of responses)[4]

68 per cent of surveyed experts believed small and medium businesses have "basic" cyber security hygiene

When asked about the federal government's cyber security maturity, there was no clear consensus



[5] Cynch (2021)
[6] McKinsey (2022)
[7] Forbes (2022), Accenture analysis

Cyber attack detection is important as attacks that go undetected lead to the highest costs

Prolonged exposure to cyber attacks increases the cost of the attacks. The longer a cyber attack goes unidentified or unresolved, the more costly it will be. The estimated cost increase of cyber attacks left unresolved for extended times ranges from 11 per cent to 35 per cent.[9,11]

The greater the disruption, the quicker an attack is detected and resolved. Disruptive cyber attacks (such as sustained disruptions to essential services and extraction of data) are the fastest to be identified of all attacks. Experts think that disruptions to essential services are on average detected in one week and resolved in two weeks. In contrast, 30 per cent of scanning and reconnaissance attacks (which are the least disruptive) are never identified or resolved. It can take almost a year (47 weeks) to detect and more than a year (53 weeks) to resolve this type of attack.

Organisations with proactive cyber security identify and resolve cyber attacks faster than those with basic maturity. According to a 2021 Accenture survey, 55 per cent of organisations with 'advanced' cyber security identify security breaches within one day and 100 per cent resolve them in 15 days or less. In comparison, only 15 per cent of organisations with basic cyber security hygiene identify security breaches within one day and only 30 per cent resolve them in 15 days or less.[11,12]

Comments

- Scanning and reconnaissance attacks take longest to be identified of all attack types, likely due to them often being imperceptible.
- In fact, over 30 per cent of experts think that these attacks are never identified or resolved.
- Note: There are no tangible costs associated with this type of attack

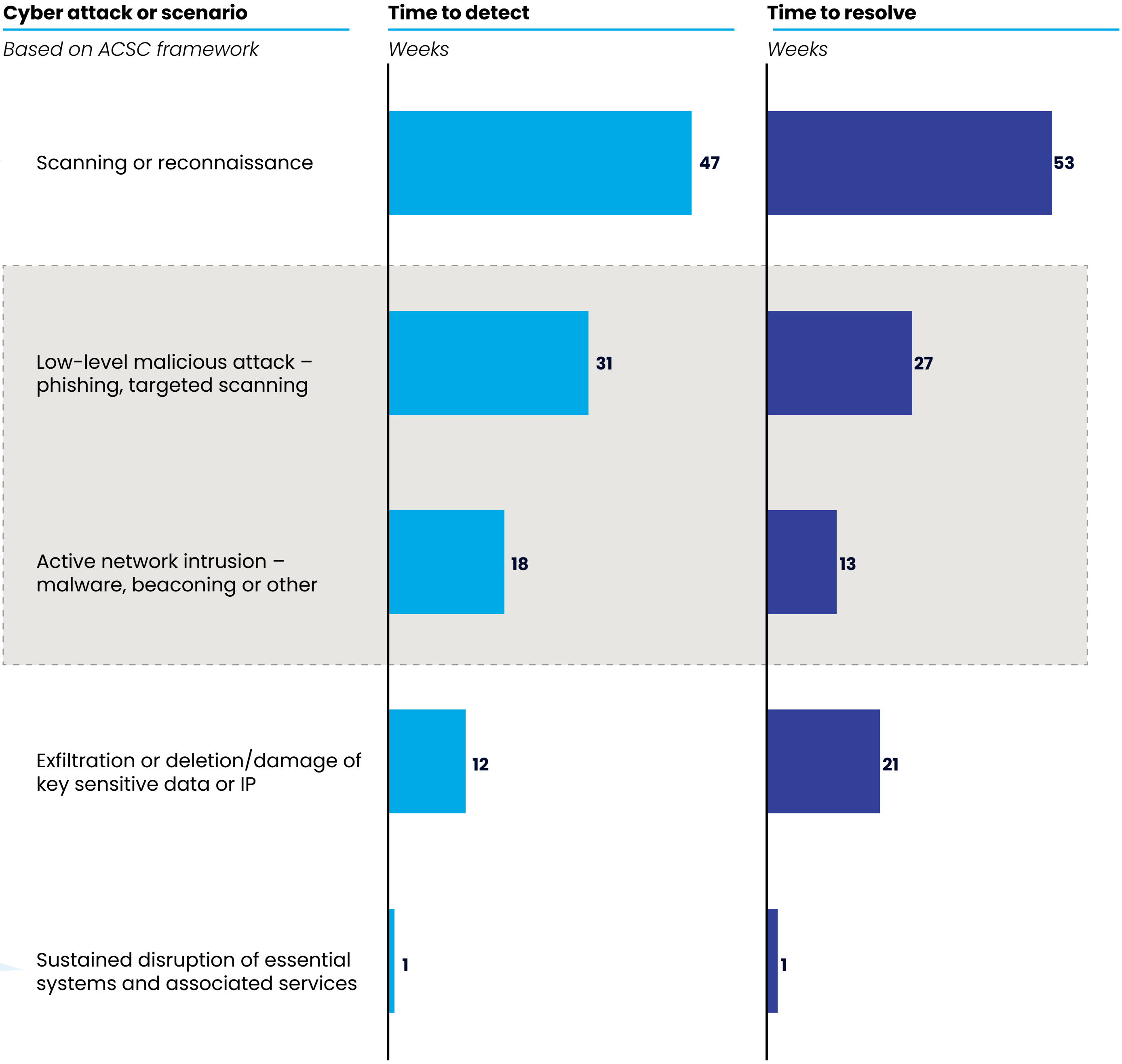
- It can take months to identify and resolve active network intrusions, such as malware.
- The longer it takes to identify and contain an attack, the more costly it is. Prolonged exposure to cyber attacks could increase the costs of an attack by 35 per cent.[1]

- Sustained disruption of essential systems and associated services are the fastest to be identified of all attack types, due to their disruptive nature.
- Unplanned downtime tied to cyber attack can cost a business $200,000 per hour.[10]

[9] IBM (2021)
[10] Splunk (2022)
[11] Accenture (2021)
[12] Expert interviews, Accenture analysis

Estimated time to detect and resolve cyber attacks according to experts

Average time to identify and remediate cyber attacks in weeks[8]



[8] AustCyber's Digital Census 2022 – "In your opinion, how long on average does it take to a) identify and b) resolve a breach/attack in each of the following scenarios?"

To understand the value cyber security provides to the economy, this report models the costs of three hypothetical attack scenarios

Scenario 1

An active network intrusion via Log4j

In Scenario 1, financially-driven malicious actors exploit the Log4j vulnerability to obtain access to computers and networks. Hackers use the vulnerability to access data and confidential files from victims.

Up to 60 per cent of firms in Australia have a Log4j vulnerability, making this scenario devastating.[13] Affected firms would be unable to use their digital infrastructure, causing huge disruption and economic losses. The impacts would vary between industries, for instance retail businesses may not be able to buy or sell goods online, while information technology firms may have to shut down their entire operation until the breach is rectified.

Why this scenario?

- The Log4j vulnerability is already being exploited by malicious actors; over 93 million Log4j-related attacks were detected in 2021.[14]
- In 2017, a widescale attack using the WannaCry Ransomware infected 230,000 systems and is estimated to have cost US$4 billion globally.[15]

Scenario 2

A sustained disruption to the electricity grid

In Scenario 2, state actors attack the IT infrastructure of an Australian electricity provider, leading to a blackout across New South Wales.

A cyber attack to New South Wales would lead to a state-wide blackout.

All households and businesses in New South Wales would be impacted by the electricity outage, experiencing downtime.

This is conservative, as an attack to the National Electricity Market (NEM) which connects the entire east coast of Australia could cause blackouts across five states.[16]

Why this scenario?

- Australia's grid is increasingly vulnerable to hackers as the electricity system becomes more complex.[17,18]
- A similar attack occurred in 2022 in Ukraine. The Ukrainian electricity grid was attacked by Russian hackers, which could have led to an outage for two million people.[19]

Scenario 3

A wide-scale low-level malicious attack

In Scenario 3, malicious actors coordinate wide-scale phishing attacks to obtain personal information and data.

Up to 60 per cent of businesses would be affected, as well as millions of households. Impacted businesses risk sensitive information being accessed and would need to update their identity verification process.

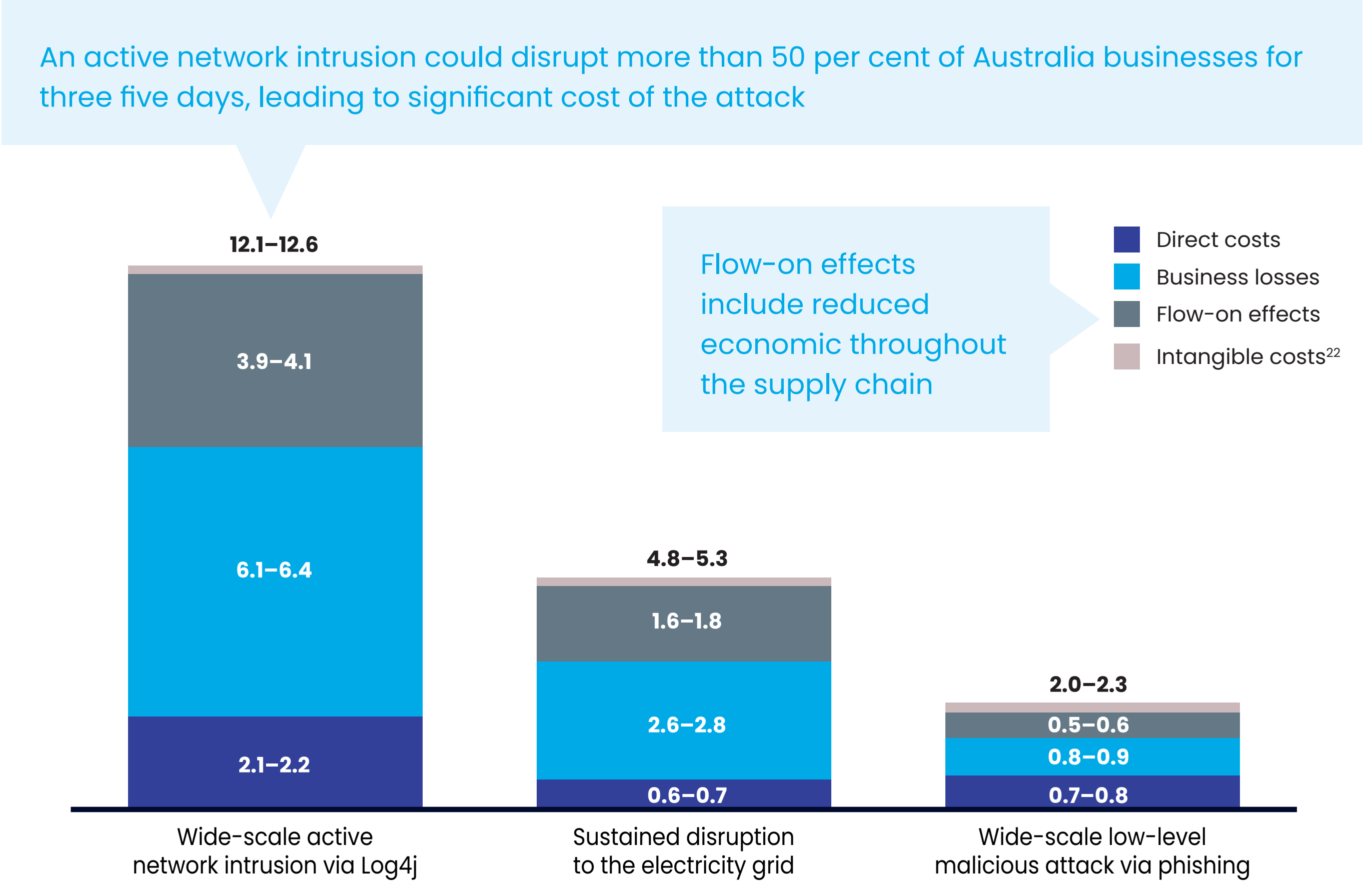
Why this scenario?

- Phishing attacks are the most reported type of cyber attack in Australia.[20] In 2021, 71,000 reports of phishing attacks were made to the ACCC.[21] Direct financial costs of phishing attacks have quadrupled between 2017 and 2021.[21]
- Phishing attacks are on the rise, with malicious actors taking advantage of health scares during COVID-19 to distribute phishing scams.

[13] AustCyber's Digital Census 2022
[14] Computer Weekly (2021)
[15] Kaspersky (2022)
[16] Guardian (2022)
[17] Trellix (2022)
[18] ABC (2022)
[19] Technology Review (2022)
[20] ACSC (2022)
[21] ACCC (2022)

A cyber attack against Australia could cost up to $12.6 billion

The potential cost of cyber attacks to Australia
A$, billions


An active network intrusion could disrupt more than 50 per cent of Australia businesses for three five days, leading to significant cost of the attack

Flow-on effects include reduced economic throughout the supply chain

Modelling assumptions

1. Wide-scale active network intrusion via Log4j

- It is assumed a wide-scale malware attack via Log4j vulnerability, estimated at 60 per cent.[2]
- The attack is assumed to reduce economic output of impacted businesses by 60 per cent, for five days.

2. Sustained disruption to the electricity grid

- It is assumed the attack will result in a black-out impacting all households and businesses in New South Wales.
- The economic output of businesses would be reduced by 100 per cent for 1.5 days.

3. Wide-scale low-level malicious attack via phishing

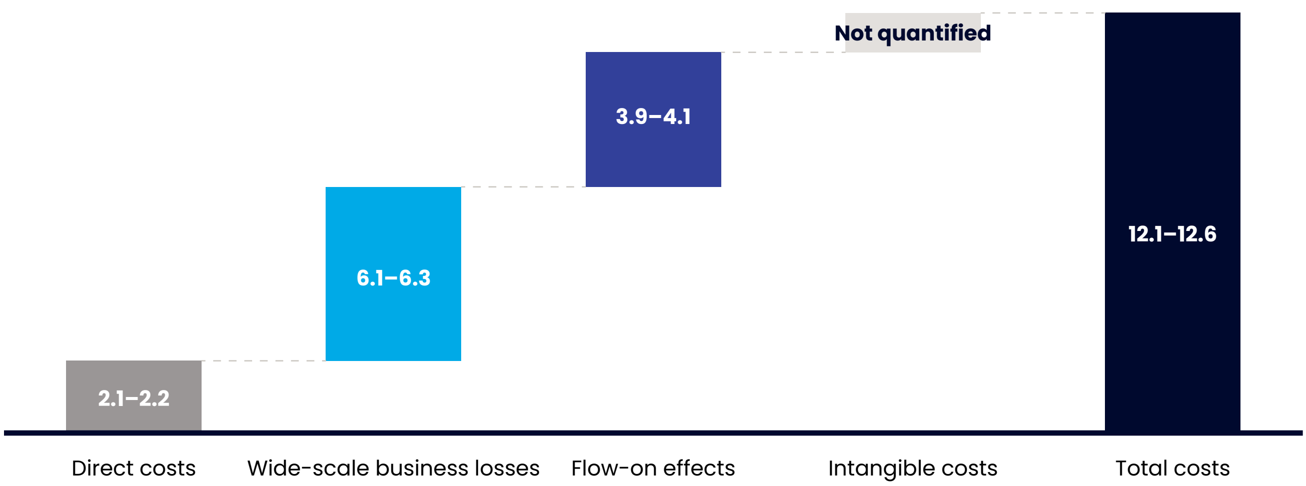
- It is assumed 70 percent of businesses would be impacted.
- Impacted businesses would be disrupted for three days, on average, reducing their economic output by 15 per cent.

[22] Intangible costs are illustrative as these cannot be quantified accurately
[2] Forbes (2022), Accenture analysis

A widescale active network intrusion via Log4j could cost up to $12.6 billion and would significantly disrupt businesses and the broader economy

Total costs of a widescale malware attack via Log4j

A$, billion



Direct costs + **Widescale business losses** + **Flow-on effects** + **Intangible costs**[22] = **Total costs**

Direct costs

Financial costs incurred from a Log4j malware attack to consumers and businesses.

Widescale business losses

Economic and supply chain costs of an attack via Log4j. These are driven by:

- Lost productivity, including lost wages and lost operating surplus
- Supply chain costs, due to disruption of the supply chain.

Flow-on effects

Intangible costs[22]

Intangible costs such as deterrence of businesses to digitalise.

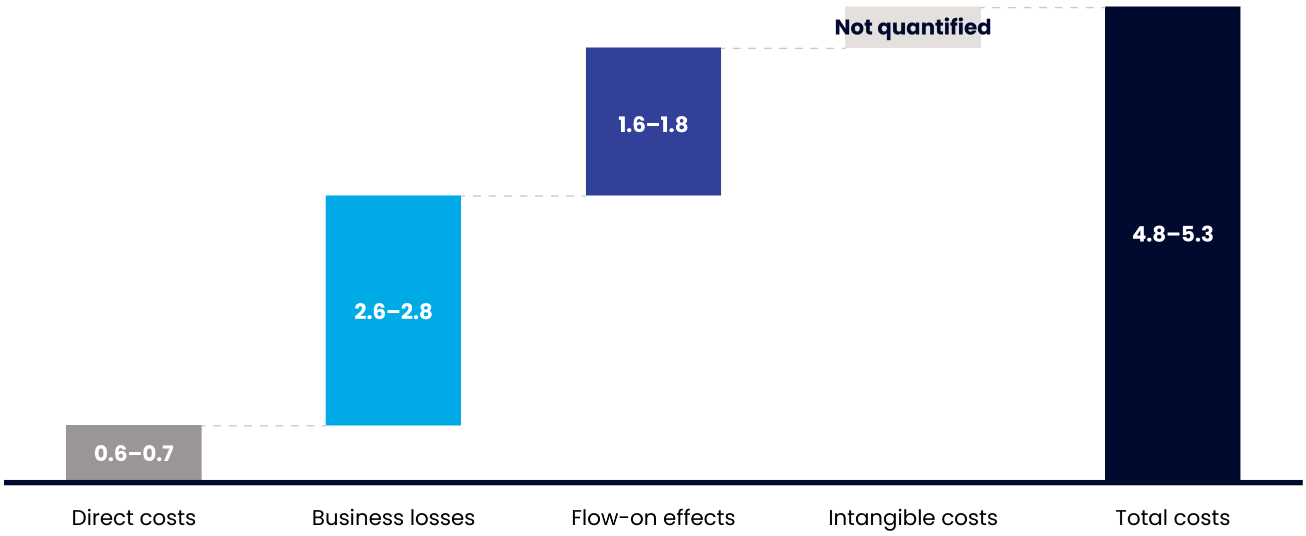
Total costs

Total costs are the costs incurred to businesses and consumers, economic and intangible costs.

[22] Intangible costs are illustrative as these cannot be quantified accurately

A single, targeted cyber attack against the electricity grid could cost the Australian economy up to $5.3 billion

Total costs of a cyber attack against the electricity grid
A$, billion



Direct costs + **Business losses** + **Flow-on effects** + **Intangible costs**[22] = **Total costs**

Direct costs

Financial costs incurred by the electricity provider from a cyber attack.

Business losses + **Flow-on effects**

Economic costs of an electricity grid disruption. These are driven by:

- Lost productivity, including lost wages and lost operating surplus
- Supply chain costs, due to disruption of the supply chain.

Intangible costs[22]

Intangible costs such as reduced access to essential services and impacts to safety.

Total costs

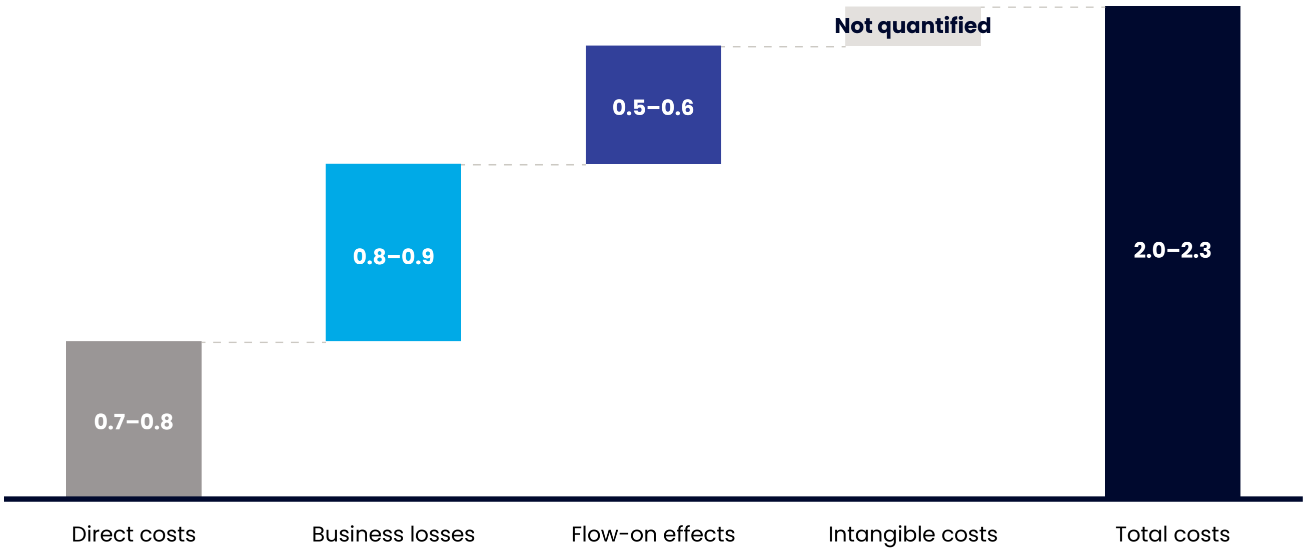
Total costs are the costs incurred to businesses and consumers, economic and intangible costs.

[22] Intangible costs are illustrative as these cannot be quantified accurately

The costs of phishing attacks could reach $2.3 billion, driven by $800 million in direct costs to remediate the attack and $900 million in business losses

Total costs of a phishing attack

A$, billion



Direct costs +

Financial costs incurred from a phishing attack to consumers and businesses.

Business losses + **Flow-on effects** +

Economic costs and supply chain disruptions incurred from a phishing attack to consumers and businesses:

- Lost productivity, including lost wages and lost operating surplus
- Flow-on effects, due to disruption of the supply chain.

Intangible costs[22] =

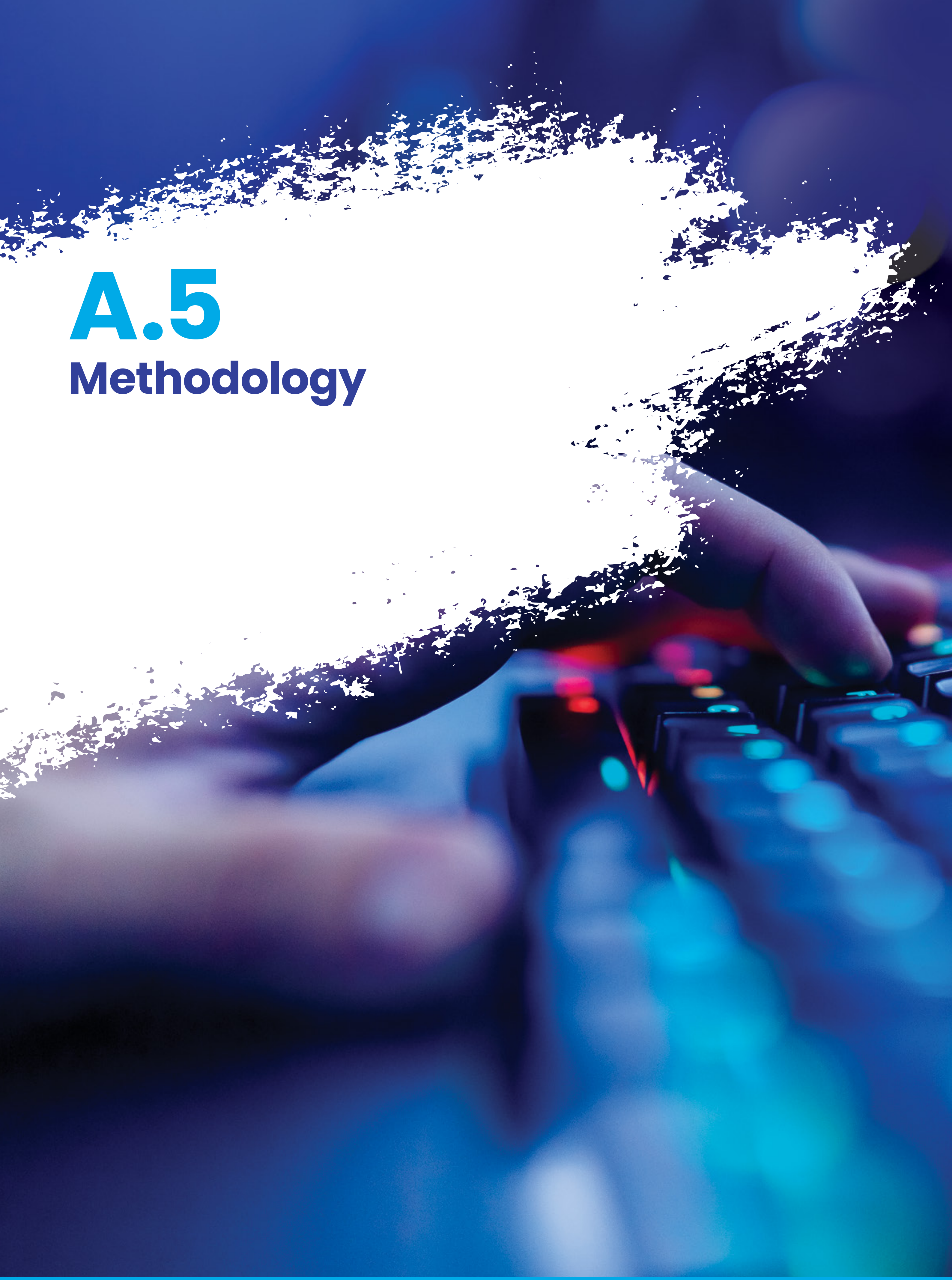
Intangible costs such as deterrence of businesses to digitalise.

Total costs

Total costs are the costs incurred to businesses and consumers, economic and intangible costs.

[22] Intangible costs are illustrative as these cannot be quantified accurately

A.5 Methodology



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] • 2020 SCP measurement model
Sector revenue	The amount of revenue that accrues to cyber security firms where their core activities take place in Australia (includes both Australian and foreign-owned firms).	• 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 security firms 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 firms 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 AustCyber's Digital Census 2022 was performed, supplemented with AUCYBERSCAPE data to fill in gaps for firms that did not respond to the survey.	• Gartner • Expert interviews • AustCyber's Digital Census 2022, n=85 • AUCYBERSCAPE
Employment	Employees in the cyber security sector, including full-time, part-time, contractor and casual workers in dedicated roles.	• The number of dedicated cyber security workers (those whose job titles reflect a pure cyber security position, such as a Cyber Security Engineer or an Information Security Analyst) in Australia was determined using AUCyberExplorer data, which is based on analysis from Lightcast (formerly Emsi Burning Glass), Accenture and CompTIA.	• AUCyberExplorer

[1] Gartner Information Security Forecast, 2016–2022 1Q22 Update

Output	Description	Approach	Data sources
Gross value added (GVA)	Measuring the cyber security sector's GVA reveals its direct contribution to the Australia's economy.	- GVA is made up of gross operating surplus and returns to workers (wages). - Sector gross operating surplus was estimated using the weighted average profit margin of about 60 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 - AustCyber's Digital Census 2022
Workers leaving the cyber security workforce	Number of workers in cyber security leaving the workforce each year.	- The ABS Census Longitudinal Dataset was used to estimate the number of cyber security workers leaving the workforce each year. - The share of ICT professionals (as a proxy for cyber security workers) in 2016 working in occupations different to where they were working in in 2011 was used to estimate the number of workers leaving the workforce to different fields. The same dataset was used to estimate the number of retiring workers each year. These were added to estimate the total number of workers leaving the cyber security workforce each year. - According to ABS data, 5.1 per cent of the ICT professionals leave the workforce each year.	- ABS Census[2]

[2] ABS Census Longitudinal Dataset (2022)

Output	Description	Approach	Data sources
New graduates and existing workers up/reskilling into cyber security	Number of graduates and existing workers entering the workforce each year.	• Measured as the number of graduates expected between now and 2026 from university degrees or VET qualifications in 'cyber security', based on average program completions between 2017 and 2021. • Course completion rate for TAFE is 46 per cent and approximately 27 per cent of students are international students and 95 per cent of students end up working in the same sector as their course.	• NCVER[3] • DESE[4] • Prosple[5] • Universities Australia[6]
Newly arrived skilled migrants	Number of skilled migrants joining Australia's cyber security workforce each year.	• Estimate based on the average number of skilled visas granted per year between 2015 and 2020 to workers in ICT occupations, defined as a subset of ANZSCO codes, assuming that a fixed proportion is for cyber security workers. • The visa subclasses for temporary and permanent migration include 186, 187, 482, 494 and 858.	• Home Affairs[7]

[3] NCVER (2022)
[4] DESE (2022)
[5] Prosple (2021)
[6] Universities Australia (2022)
[7] Home Affairs (2022)

Speed
37 Gb/s

AustCyber
Part of the Stone & Chalk Group.

Contact

Email:	info@austcyber.com
Website:	www.austcyber.com
Twitter:	@AustCyber

Scan here to view the SCP online