



Australia's Cyber Security Sector Competitiveness Plan 2023

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

Plan at a glance

2023 highlights

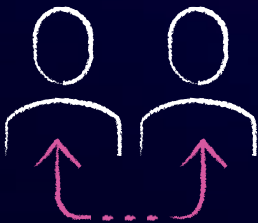
Growth



Australia's cyber security sector contributed an estimated **AU\$6.9 billion** to the country's Gross Domestic Product (GDP)¹.



The Gross Value Added (GVA) of the cyber security sector to the Australian economy increased by approximately **60 percent** from AU\$2.44 billion in 2022 to approximately AU\$3.99 billion².



There are over **315** cyber security companies in Australia³, an increase of **8.25 percent** from 2022, with the average age being 5.5 years.



50 percent of cyber security companies are exporting globally.

¹ Oxford Economics Australia analysis

² Oxford Economics Australia analysis

³ AUCyberscape

Workforce

A total of **125,791 people** were employed in the Australian cyber security workforce in 2022⁴.

51,309 were identified as Dedicated Roles (41%), an estimated increase of 9.5 percent since the previous year⁵.

Of the Dedicated Roles, **24,254** were identified as Core Roles, requiring technical expertise (19%)⁶.

74,482 were identified as Related Roles (59%) requiring cyber skills knowledge⁷.



17 percent of the workforce identify as female in cyber security⁸ compared to **0.66 percent** identifying as being of Aboriginal and/or Torres Strait Islander heritage and **7 percent** identifying as neurodivergent in the technology sector⁹.

The salaries of Australian advertised cyber security positions in the private sector averaged **AU\$124,331**. The equivalent in the public sector was **AU\$119,694**¹⁰.

Since 2019, enrolments in security science degrees¹¹ have increased by **30 percent per annum**¹².



The global cyber security workforce reached a historic high of **5.5 million professionals**, marking an increase of 440,000 positions compared to 2022, representing an 8.7 percent surge¹³.

⁴ AUCyberExplorer, dated February 2023

⁵ Oxford Economics Australia analysis, ABS Census Data 2021

⁶ Oxford Economics Australia analysis, ABS Census Data 2021

⁷ Oxford Economics analysis, ABS Census Data 2021

⁸ Gender dimensions of the Australian cyber security sector report. RMIT, AWSN 2023

⁹ ACS Australia's Digital Pulse 2022

¹⁰ Oxford Economics Australia analysis

¹¹ Security Science degrees explained, Insider Guides, 2022

¹² Based on the Australian Standard Classification of Education (ASCED) code 029901. This code is focused only on security science related to information technology. Given its relatively limited scope, it is not likely to capture all the enrolments in the sector, so this growth number should be considered as a lower bound estimate.

¹³ ISC2 Cyber Security Workforce Study 2023

2023 highlights

Cybercrime



Australia experienced an estimated **94,000** cybercrime reports (on average 1 report every 6 minutes) in 2022–2023, an increase from 1 report every 7 minutes compared to the previous financial year¹⁴.



The cost of cybercrime to businesses increased by **14 percent** during the 2022–23 financial year. Small businesses experienced an average financial loss of **\$46,000**, medium businesses an average of **\$97,200** and large businesses an average of **\$71,600**¹⁵.

¹⁴ ASD Cyber Threat Report 2022–2023

¹⁵ ASD Cyber Threat Report 2022–2023

Outlook for 2030



The Australian cyber security sector GVA can potentially contribute an additional 32 percent to the Australian economy by 2030.

Based upon the current pace of growth, the GVA of the Australian cyber security sector is forecast to be AU\$5.2 billion by 2030¹⁶.

The Australian cyber security sector could be home to an estimated 500 sovereign companies by 2030¹⁷.



The Australian cyber security sector will require an additional 4,813 Dedicated Roles each year to meet the demand for 2030.

The Australian cyber security sector will potentially need 85,000 Dedicated Roles by 2030, an increase of 66 percent from 2023¹⁸.



To remain globally competitive, Australia must improve its support for:

- cyber security startups and the commercialisation of their sovereign technology;
- domestic procurement of Australian cyber security products and services;
- public-private partnerships to attract and upskill cyber security talent; and
- attracting investment into a rapidly maturing industry.

¹⁶ Oxford Economics Australia analysis

¹⁷ Oxford Economics Australia analysis

¹⁸ Oxford Economics Australia analysis

Foreword

Globally, 2023 was met with a dynamic geopolitical landscape, an accelerating cyber arms race and global economic uncertainties. Nationally, natural disasters impacted our country's ability to connect and many of our ASX listed companies and critical infrastructure providers were subject to cyber attacks, causing a ripple effect across all market segments and concern amongst the community.

The necessity to prioritise and invest in cyber security has never been more pronounced to protect our economy and its assets – from our nation's security and communities' personally identifiable information, to the livelihood of our small businesses.

I am pleased to present the sixth edition of Australia's Cyber Security Sector Competitiveness Plan (SCP), developed in consultation with industry, federal and state/territory governments, academics and leading industry experts who have generously shared their time and knowledge for the development of the 2023 edition.

The SCP continues to be AustCyber's flagship publication designed to help shape, inform and grow Australia's vibrant and globally competitive cyber security sector. It is a resource that continues to be cited on national and international stages when referring to the Australian cyber security sector and this edition is no different.

The 2023 edition has been developed with three key factors in mind – the release of the 2023–2030 Australian Cyber Security Strategy (the Strategy); a cyber security sector that can no longer be classified as emerging, but more so maturing; and the maturity of the data now available.

The Strategy, backed by a AU\$586.9 million investment, lays a foundational blueprint for enhancing Australia's cyber security posture. A conscious decision was made to delay the publication of the 2023 SCP, awaiting the release of the Strategy, as its impact has a direct bearing on the outlook of the cyber security industry.

The Strategy's presentation across six shields and three horizons provides a strong roadmap for government's priorities and investments; and is referred to in many instances within the SCP. From areas of focus and co-design approaches with industry, to the quantum of funding, the Strategy marks a significant step towards fortifying Australia's digital landscape.

However, for the Strategy to be truly effective, it requires a more targeted approach, especially in areas like supporting small businesses, fostering a skilled cyber workforce and more importantly, mandating cyber security standards. AustCyber is committed to working collaboratively with government and industry stakeholders to refine and implement these critical initiatives, ensuring that Australia not only meets its cyber security goals, but sets a global benchmark in cyber resilience.

As part of the 2023 edition and where possible, we have provided the reported growth of certain data sets from all six editions of the SCP. It is time we all understood the trajectory of growth from Australia's youngest economic sector – it can no longer be classified as emerging as attested to by the data presented in this SCP. A clear view of the maturity and size of Australia's cyber security sector is essential for strategic growth. Good policy and future investments are contingent upon policymakers, entrepreneurs and investors having a clear picture of the sector on which to make informed decisions.

As part of understanding the cyber security sector growth and future demands, the significance of data accuracy and currency cannot be overstated. Cyber security, which cuts across all sectors and industries, serves as both a business endeavour and an economic driver. This encompasses not only entities within the cyber security sector that offer specialised capabilities, but also organisations across diverse sectors that maintain in-house cyber security staff.

In our exploration of this multifaceted landscape, the precision and up-to-date nature of our data has become paramount. This SCP has transitioned from reporting data sets of ‘the cyber security workforce’ to a truer data set of economic value – Core, Dedicated and Related Roles, which has been defined in the methodology section of the SCP. This is a significant milestone in solving measurement challenges for the cyber security workforce by providing a better breakdown of employment and skills gaps in the sector.

Addressing cyber security workforce measurement complexities through innovative methodologies will empower all of us to craft resilient and nuanced industry workforce development strategies. It will also foster increased investments within the sector and provide cyber security companies with clearer comprehension of their commercial ecosystem, enabling them to seize opportunities with greater precision and insight.

From the perspective of this SCP, the global dynamics underscore the need for Australia to embed a comprehensive and adaptive approach to cyber security moving forward. The SCP explores the multifaceted approach Australia has already embraced to confront and mitigate the complex and dynamic challenges of the digital age. As we traverse this complex digital terrain, Australia stands poised to meet the challenges head-on, fortifying its cyber security defences and pioneering solutions that safeguard the nation's digital future.

Chris Kirk
Chief Executive Officer
Stone and Chalk Group and AustCyber



// This SCP has transitioned from reporting data sets of ‘the cyber security workforce’ to a truer data set of economic value.”

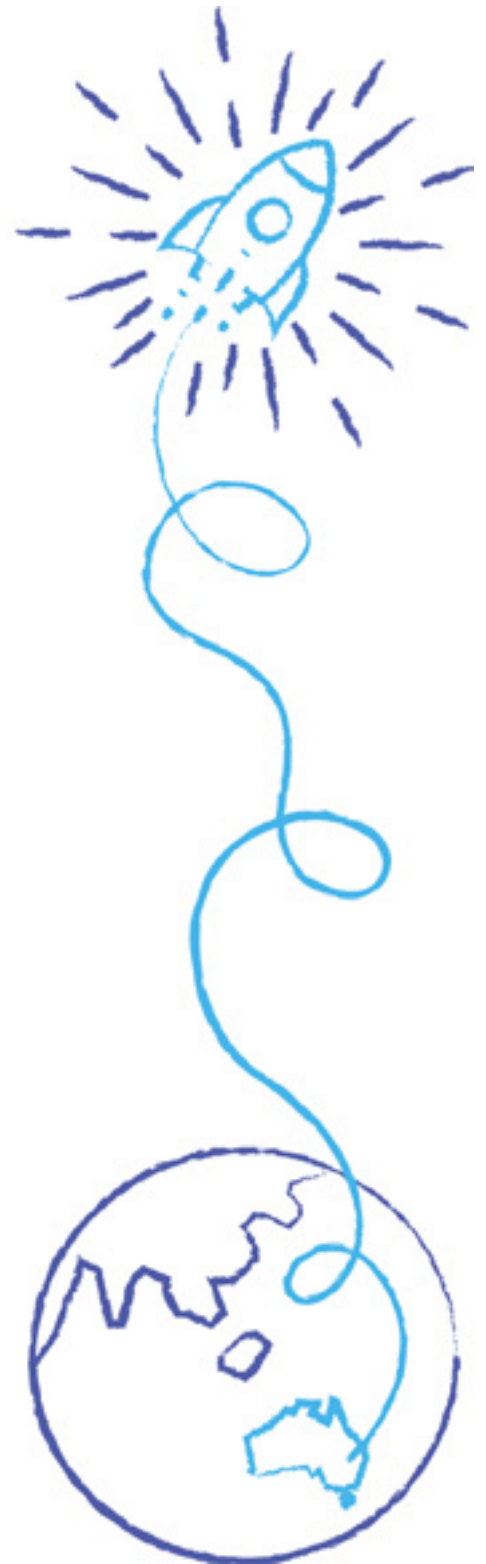
Acknowledgements

AustCyber conducted the 2023 Australian's Cyber Security Sector Survey, as well as 1:1 interviews with government, the private sector and research community in both Australia and internationally to inform the detailed insights and case studies presented in this SCP.

AustCyber gratefully acknowledges and thanks all who contributed, including:

- ACT, NSW, QLD, SA, TAS, NT, VIC and WA Governments
- Austrade
- Australian Computer Society (ACS)
- Australian Cyber Collaboration Centre (ACCC)
- Australian Information Industry Association (AIIA)
- Australian Public Service Commission (APSC)
- Australian Women in Security Network (AWSN)
- Blackberry
- CSIRO Data61
- CISO Lens
- Cybermerc
- CyberMindz
- CyRise
- CloudShare
- Cyber Security Cooperative Research Centre (CSCRC)
- Department of Industry, Science and Resources
- IoT Alliance Australia
- KordaMentha
- RMIT University
- TAFECyber
- The University of Melbourne
- University of New South Wales (UNSW)

AustCyber also acknowledges the significant contributions made by Oxford Economics Australia for the provision, collection and analysis of economic data; as well as Cygenus in the drafting of this SCP.



Contents

Executive summary	2
Highlights the key findings of this Sector Competitiveness Plan.	
Chapter 1: The global outlook for cyber security	4
Describes the global outlook of the international cyber security market – including revenue, cybercrime, workforce and trends. It also provides a comparative view of national cyber security strategies.	
Chapter 2: Potential growth opportunities for Australia	16
Outlines the 2023 global positioning of Australia, the national economic value, its growth to date and government investment into the industry.	
Chapter 3: Challenges to sector growth	34
Describes the challenges to sector growth focusing on economic, labour and ecosystem environments.	
Chapter 4: Actions to build a more competitive cyber security sector	42
Provides a special edition analysis of the 2023–2030 Australia’s Cyber Security Strategy and recommends actions to build a more competitive cyber security sector.	
Chapter 5: The role of AustCyber	56
Explains the activities and actions undertaken by AustCyber in supporting the development of a vibrant and globally competitive Australian cyber security sector.	
Appendix A: State of the states	61
Provides an overview and initiatives undertaken by each Australian state and territory.	
Appendix B: Cyber security taxonomy	70
Provides a list of cyber security product and service categories and their definitions.	
Appendix C: Methodology	73
Outlines the methodologies utilised in drawing together the data for the SCP.	

Executive summary

The Australian cyber security sector in 2023 was characterised by significant growth, evolving challenges and a compelling need for strategic investments to maintain global competitiveness.

The Australian cyber security sector stands at a pivotal juncture, shaped by a rapidly digitising economy and escalating global threats. The economic value of this sector is undeniable, yet there remains a stark contrast in its growth trajectory when compared to its global peers.

Digitalisation trends, amplified by the rapid adoption of artificial intelligence, have skyrocketed the demand for robust cyber security solutions across all industries. This surge underlines the sector's critical role in ensuring digital trust, promoting economic growth and shielding our intricate digital value chains.

The strategic focus must be on aligning with secure-by-design principles, connecting security with digital technology development and value chain expansion. The sector must embrace innovation, invest in public-private partnerships and address the education and workforce challenge.

In 2004, the global cyber security market was worth US\$3.5 billion and now it's one of the largest and fastest-growing sectors in the information economy. The cyber security market is expected to grow by 15 percent year-over-year from 2021 to 2025¹⁹.

What was once considered the future of cyber security, has now solidified into a tangible present, fundamentally reshaping the way we must view Australia's contribution on a global scale in terms of technology, innovation, research and development, and its sovereignty to capture the global market.

The Australian cyber security sector growth and economic contribution in 2023 signified its growing economic importance, adding approximately AU\$6.9 billion to the country's Gross Domestic Product (GDP) and AU\$3.99 billion in Gross Value Add (GVA).

The sector witnessed a notable increase in the number of companies, with over 315 cyber security companies in Australia, showcasing resilience and entrepreneurship in the field.

Notably, 50 percent of these companies are actively exporting cyber security products and services globally, contributing to Australia's international presence²⁰.

The workforce in the cyber security sector continued to grow with over 51,000 cyber security professionals in Dedicated Roles that demand cyber security technical skills or knowledge. Despite progress, gender diversity in the cyber security sector remains a challenge, with only 17 percent of the current cyber security workforce identifying as female. This is significantly lower for those who identify as Aboriginal and/or Torres Strait Islander heritage or neurodivergent.

¹⁹ Cybersecurity Ventures, 2023

²⁰ AUCyberscape as at 31 December 2023

Looking ahead to 2030, the GVA of the Australian cyber security sector is projected to reach AU\$5.2 billion, necessitating continued investment and innovation.

The sector is poised for substantial expansion, with a potential 500 sovereign companies by 2030, reinforcing Australia's presence in the global cyber security arena.

To meet the evolving demands of the sector, an estimated 85,000 Dedicated Roles will be needed by 2030, underlining the importance of talent development and upskilling initiatives.

With strategic investments and a commitment to innovation, Australia is well-positioned to secure its digital future and play a pivotal role in the global cyber security ecosystem.

2023 demonstrated that the cyber security industry exhibits robust growth and potential, coupled with persistent challenges. To remain globally competitive, Australia must prioritise support for startups, domestic procurement and public-private partnerships, all while addressing the evolving threat landscape.



Chapter 1: The global outlook for cyber security



On a global scale, 2023 emerges as a pivotal moment in cyber security.

Rapid proliferation of interconnected devices has broadened the attack surface for cyber criminals; unprecedented convergence of technologies such as artificial intelligence (AI) and machine learning (ML) are increasingly being integrated into cyber security systems; and Advanced Persistent Threats (APTs) are becoming more prevalent targeting critical infrastructure as the escalation of a 'cyber arms race' sees governments worldwide build enduring advantages in cyberspace²¹. With prominent data breaches underscoring the urgency for governments worldwide to legislate and regulate the safeguarding of personal identifiable information, the global cyber security landscape stands at a critical juncture.

Global revenue

Against the backdrop of growing concerns about data vulnerabilities and cyber threats, the global cyber security landscape has experienced significant expansion in recent years. With the ongoing effects of the COVID-19 pandemic, combined with the use of cyber capabilities during the Russia-Ukraine conflict, revenue in the global cyber security market surged from approximately US\$83.32 billion in 2016 to around US\$166 billion in 2023²².

In addition to the significant developments on a global scale, acceleration in the prioritisation and spending in cyber security is evident, reflecting a substantial increase in demand for cyber defences and protection. In a global comparison, most revenue will be generated in the United States (US\$72 billion), followed by China (US\$13 billion) and the UK (US\$10 billion) in 2023, with Australia reaching US\$3.8 billion.

Global revenue is expected to show an annual growth rate (CAGR 2023–2028) of 10.48 percent, resulting in a market volume of US\$273.60 billion by 2028.

In 2023, Australia is ranked seventh globally in terms of revenue growth rate, in comparison to 2022 where it was ranked ninth globally.



²¹ United Nations General Assembly First Committee October 2023 (GA/DIS/3725)

²² Cybersecurity market data and analysis, Statista, November 2023

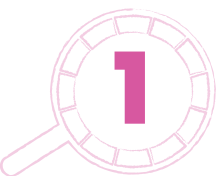
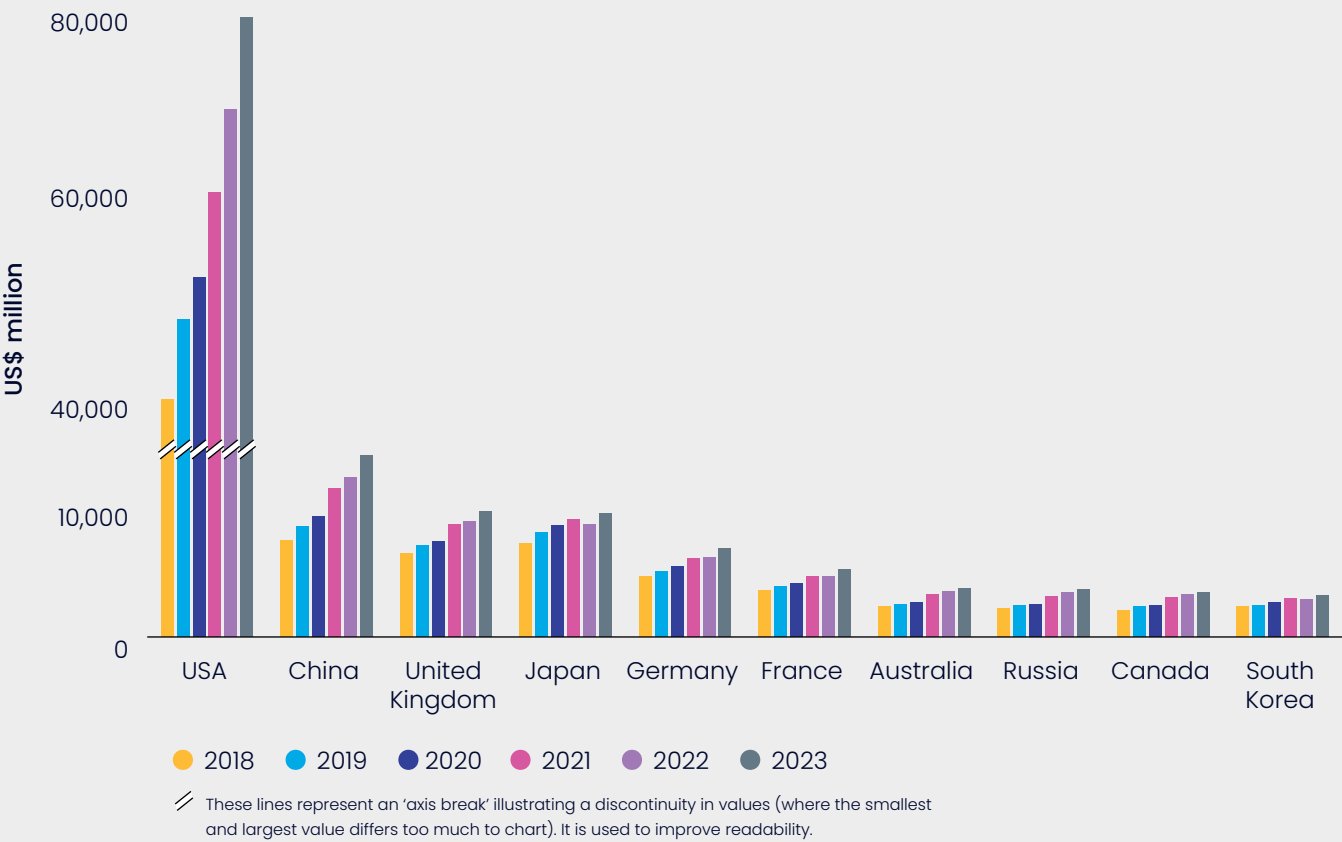


Figure 1. Average annual revenue growth rate between 2018 and 2023 (US\$ million)²³

	2018	2019	2020	2021	2022	2023
USA	42,960	49,010	52,150	58,560	64,860	71,790
China	7,283	8,351	9,134	11,220	12,050	13,710
United Kingdom	6,319	6,913	7,208	8,493	8,742	9,445
Japan	7,044	7,870	8,391	8,900	8,520	9,319
Germany	4,577	4,957	5,325	5,920	5,996	6,677
France	3,535	3,825	4,033	4,603	4,606	5,090
Australia	2,269	2,451	2,607	3,246	3,452	3,638
Russia	2,141	2,415	2,418	3,037	3,352	3,561
Canada	2,036	2,268	2,363	2,963	3,238	3,340
South Korea	2,273	2,414	2,589	2,890	2,852	3,102



23 Statista Market Insights September 2023

Global cybercrime²⁴

The interconnected nature of the global economy means that a cyber incident in one country can have far-reaching and cascading effects on others. The cost of global cybercrime has increased by an estimated 176.27 percent from US\$2.95 trillion in 2020 to US\$8.15 trillion in 2023. It is expected to reach US\$13.82 trillion by 2028.

Globally, cyber attacks surged to a peak in 2021, reaching 19.23 million recorded incidents. This marks a 6.5 percent increase from the previous year. However, there has been a notable reduction in 2022, with recorded cyber attacks totalling 16.8 million. This represents a significant decrease of 14.5 percent compared to 2021. It is suggested that the reduction may be due to the adoption of cyber security post the COVID-19 pandemic in both developing and developed countries. Among these incidents, phishing scams constituted a significant 53 percent, while personal data breaches accounted for 10 percent of the recorded cyber attacks. These statistics illuminate the wide spectrum of threats confronting both organisations and individuals throughout the year 2022.

Figure 2. 2022 Global cybercrime by type (%)²⁵



²⁴ Statista Market Insights September 2023

²⁵ Statista Market Insights September 2023

Global workforce

The global cyber security workforce has achieved unprecedented growth, but the persistent demand for skilled cyber professionals continues to outstrip the available talent pool. This shortage is particularly pronounced in areas such as cloud security, artificial intelligence and machine learning expertise in cyber security, zero-trust architectures and the ability to effectively troubleshoot and communicate.

In 2023, the global cyber security workforce reached a historic high of 5.5 million professionals, marking a remarkable increase of 440,000 positions compared to 2022, representing an 8.7 percent surge.

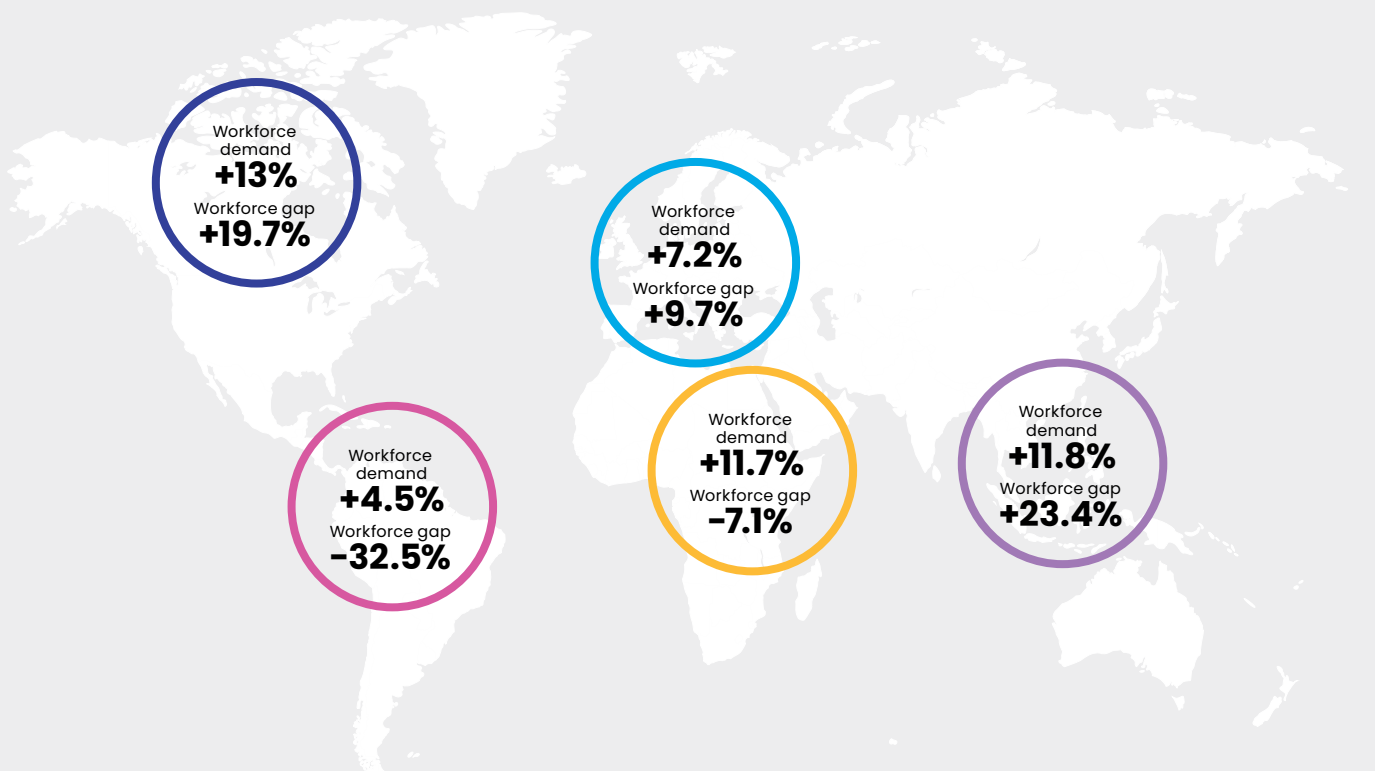
While this growth is commendable, it exists in the shadow of persistent unmet demand. In 2022, the gap between global workforce supply and cyber security workforce demand was estimated at 3.4 million. The gap between the number of professionals needed and the number available has continued to grow, with a 12.6 percent increase year on year.

Figure 3. 2023 Global cyber security workforce demand²⁶

North America	Latin America	Europe	Middle East & Africa	Asia-Pacific
1,495,825 (+13%)	1,285,505 (+4.5%)	1,309,588 (+7.2%)	401,582 (+11.7%)	960,231 (+11.8%)

Figure 4. 2023 Global cyber security workforce gap

North America	Latin America	Europe	Middle East & Africa	Asia-Pacific
521,827 (+19.7%)	348,259 (-32.5%)	347,761 (+9.7%)	111,801 (-7.1%)	2,670,316 (+23.4%)



²⁶ ISC2 Cyber Security Workforce Study 2023

Global partnerships and strategies

With an exponential increase in the volume of data collected and shared across international partnerships, governments are driven by the imperative to protect critical infrastructure, safeguard national security, ensure data privacy and adapt to evolving cyber threats.

This is of particular importance closer to home. The AUKUS deal – a trilateral security partnership between Australia, the United Kingdom and the United States – involves various aspects of defence and security cooperation with Australia. The announcement of the AUKUS deal in 2021 drew significant attention and discussions regarding the regional security dynamics in the Indo-Pacific region. Cyber security is a crucial component of the AUKUS deal as it directly impacts the protection of critical assets, exchange of sensitive information, resilience against cyber threats and the overall security posture of the partnership. To fully realise the objective of the AUKUS agreement, the member countries must prioritise and collaborate on cyber security measures to protect their shared interests and capabilities.

This is evidenced through the formulation and execution of National Cyber Security Strategies for nations worldwide. A comparative review of cyber security strategies (across Australia, United Kingdom, United States, Canada and New Zealand) provides insights into the prioritisation and spending on cyber security, as well as collaboration across global partnerships.

Although each country has its specific regional and national context, the strategies consider the cyber threat landscape and wider global context. However, there are some common priority areas:

- legislative and regulatory approaches to cyber policies as binding obligations rather than voluntary standards;
- greater protection of critical national infrastructure across all sectors;
- addressing the shortage of cyber professionals amidst international events, trends and global competition; and
- engagement in multilateral and bilateral agreements for cyberspace norms.

Investment in National Cyber Security Strategies varies significantly on a per capita basis; from US\$0.97 in New Zealand to US\$41.56 for the United Kingdom. However, the context behind each strategy may shine a light on the disparity in investment – New Zealand's Cyber Security Strategy 2019 has been described as 'guiding principles' to maintain its cyber security, whilst the United Kingdom is the third most targeted country in the world for cyber attacks, after the US and Ukraine²⁷.

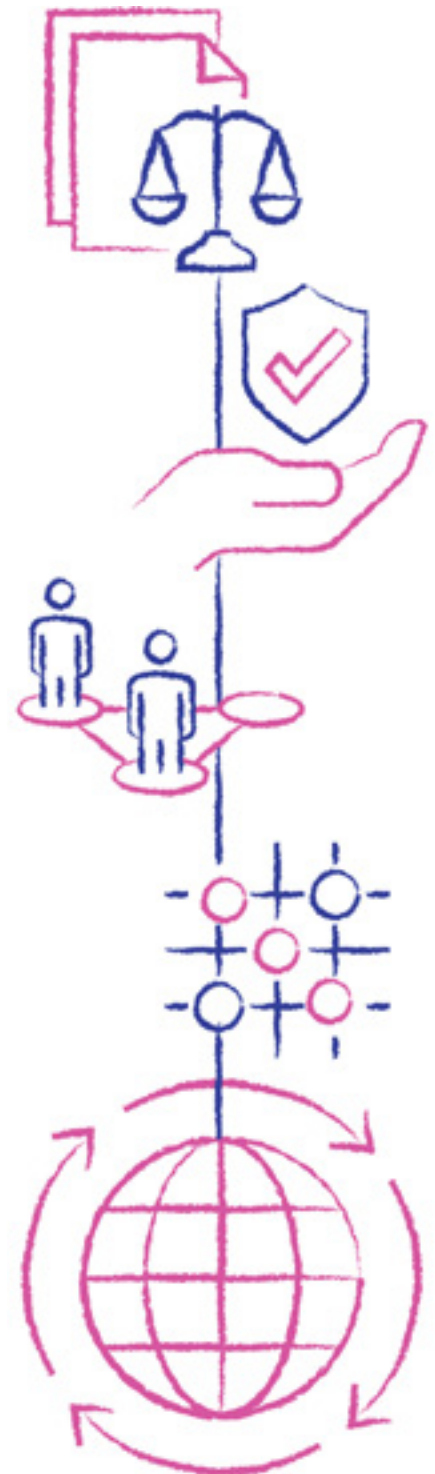


Figure 5. Review of National Cyber Security Strategies

Note: The respective investment amounts reflect the publicly highlighted figures and capture different spends.

	Australia	United Kingdom ²⁸
Period	2023–2030	2022–2030
Investment (US\$)	\$402.21 million \$15.10 per capita	\$2.78 billion \$41.56 per capita
Priorities	Six shields: <ul style="list-style-type: none">• Strong business and citizens• Safe technology• World-class threat sharing and blocking• Protected critical infrastructure• Sovereign capabilities• Resilient region global leadership	Five pillars: <ul style="list-style-type: none">• Strengthening the UK cyber ecosystem• Building cyber resilience• Taking the technology advantage• Advancing UK global leadership• Countering cyber threats to the UK
Supplementary government publications	Australia’s National Cyber Security Action Plan 2023–2030	Government Cyber Security Strategy 2022–2030

28 National Cyber Strategy 2022



United States ²⁹	Canada ³⁰	New Zealand ³¹
2023–2030	2018–2023	2019–2023
Unavailable	\$384.7 million	\$5.08 million
	\$9.92 per capita	\$0.97 per capita
Five pillars: <ul style="list-style-type: none"> • Defend critical infrastructure • Disrupt and dismantle threat actors • Shape market forces to drive security and resilience • Invest in a resilient future • Forge international partnerships to pursue shared goals 	Three themes: <ul style="list-style-type: none"> • Security and resilience • Cyber innovation • Leadership and collaboration 	Five priorities: <ul style="list-style-type: none"> • Cyber security aware and active citizens • Strong and capable cyber security workforce and ecosystem • Resilient and responsive New Zealand • Proactively tackle cybercrime • Internationally active
National Cyber Workforce and education strategy roadmap 2023 Department of Defence Cyber Strategy	National Cyber Security Action Plan 2019–2024	

29 National Cyber Security Strategy 2023

30 National Cyber Security Strategy

31 New Zealand's Cyber Security Strategy 2019



Global trends³²

Cyber threats

As digital and technological advancements persist, so do the evolving threat vectors. Phishing attacks maintain their position as the most prevalent form of cybercrime, with a growing concern over the rise of mobile phishing attacks, including 'smishing' and 'quishing'. Network intrusions, including the menacing presence of ransomware, continue to pose significant threats to both governments and businesses. It's important to emphasise that the primary motivation behind these attacks appears to be centred around business disruption, reputational harm or the potential 'collateral damage' within supply chains.

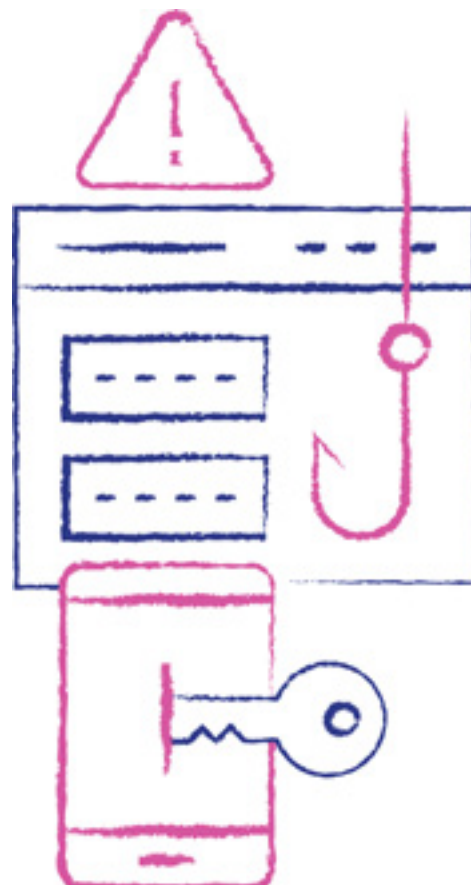
Technological advancements

The rapid progression and widespread adoption of AI and ML technologies, as well as cloud-based technologies, evoke both hope and concern. Substantial advancements will continue to occur in cyber security as AI can be a force multiplier – AI and automation can move resources from detection capabilities to more strategic roles. However, the downside of AI is its potential to fuel innovation in cybercrime, where malicious actors will continue to exploit these technologies. Furthermore, the autonomous learning capabilities of ML models raise concerns about their potential misuse. There exists a prevailing ambiguity regarding the strategies governments, corporations and communities will employ to ensure the safe and ethical development, deployment and oversight of AI and other tech-based systems. This continues to be an issue grappled at every level of government.

Laws and regulations

As cyber threats continue to evolve, so too is the legal and regulatory framework governing cyber security practices, albeit at a much slower pace. The cyber landscape is undergoing a profound transformation in terms of laws and regulations, particularly concerning data privacy and cyber security practices.

Governments around the world are increasingly recognising the critical importance of safeguarding personal and sensitive information. Consequently, there has been a surge in the implementation of stringent data protection laws and regulations, such as the European Union's General Data Protection Regulation and the California Consumer Privacy Act. These laws empower individuals with more control over their data and impose hefty fines on organisations that fail to comply. In addition to data privacy, mandatory reporting and breach notifications have become cornerstones of modern cyber security regulations. Many countries now require organisations to promptly report data breaches to authorities and affected individuals.



³² WEF Global Cyber Security Outlook 2023, Deloitte 2023 Global Future of Cyber Survey



ChatGPT

The impact of ChatGPT on cyber security

In 2023, ChatGPT emerged as a powerful tool for various applications, including customer support, content generation and more. Launched in November 2022, ChatGPT has redefined the use of AI. As an AI chatbot built on top of OpenAI's foundational large language models (LLMs), it has redefined the standards of artificial intelligence, proving that machines can indeed 'learn' the complexities of human language and interaction.

With any new viral technology, questions have been raised. What are the cyber security implications of ChatGPT? The advantages and disadvantages? Can it help bolster defences against cyber threats? ChatGPT was asked these questions and its responses are below:

Advantages

Threat intelligence and analysis:

- ChatGPT can process vast amounts of text data, allowing it to analyse and extract valuable threat intelligence from various sources, including news articles, forums and dark web chatter.
- It helps cyber security professionals stay informed about emerging threats, vulnerabilities and trends in real-time.

Automated phishing detection:

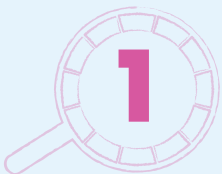
- ChatGPT can be deployed to identify and respond to phishing attempts in real-time by analysing incoming emails or messages for suspicious content and patterns.
- This automation reduces the response time to phishing attacks, minimising the risk of successful breaches.

Security awareness training:

- ChatGPT can generate tailored cyber security awareness training content for employees, providing ongoing education and best practices.
- This helps organisations improve the security posture of their workforce and reduce the likelihood of human error-related security incidents.

Incident response assistance:

- ChatGPT can assist cyber security teams in incident response by providing guidance on how to contain, mitigate and recover from security incidents.
- It offers quick access to relevant information and procedures during high-stress situations.



Disadvantages

Attack vector potential:

- Malicious actors could exploit ChatGPT's capabilities to craft more convincing phishing messages or social engineering attacks.
- The technology itself could become a potential attack vector if not adequately secured.

Bias and misinformation:

- ChatGPT may inadvertently generate biased or inaccurate information, which could negatively impact decision-making in cyber security incidents.
- The model's responses are based on the data it was trained on, which may contain biases present in the training data.

Complexity and maintenance:

- Implementing ChatGPT for cyber security requires substantial technical expertise and resources.
- Ongoing maintenance and fine-tuning of the model are necessary to ensure its effectiveness and relevance.

Human dependency:

- Over reliance on ChatGPT for critical cyber security tasks may lead to a lack of human oversight and judgment, potentially overlooking nuanced threats.

ChatGPT presents both significant advantages and challenges when applied to the field of cyber security. Its ability to analyse and generate insights from vast amounts of data, automate certain tasks and assist in incident response holds promise for enhancing cyber security practices. However, organisations must also be mindful of its potential misuse, biases and the need for human expertise and oversight in complex security environments. The successful integration of ChatGPT into cyber security strategies will require a careful balance between leveraging its advantages and mitigating its disadvantages.





Leading the charge: Australia's role as Global Chair in the establishment of the International Counter Ransomware Taskforce

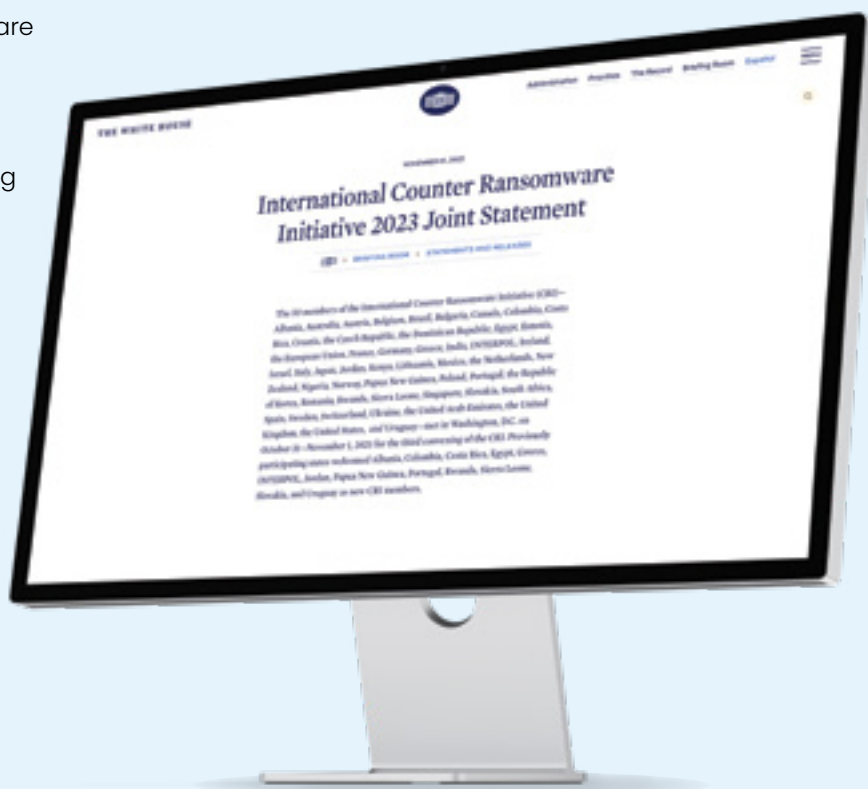
The proliferation of ransomware attacks in recent years has posed a severe threat to global cyber security, disrupting critical infrastructure, businesses and individuals alike. As part of the United States led Counter Ransomware Initiative (CRI), Australia assumed a pivotal role as the inaugural global Chair of the International Counter Ransomware Taskforce (ICRTF) in 2023.

The Taskforce was established under the Department of Home Affairs' Cyber and Critical Technology Coordination Centre, coordinating Australia's lines of effort among the members of the ICRTF.

The ICRTF builds on the activities undertaken by the CRI, and will translate this groundwork into decisive results – including cross-sectoral tools, cyber threat intelligence exchanges and collective best practice guidance for countering ransomware. The ICRTF will also act as the way through which the CRI connects with industry for defensive and disruptive threat sharing and actions.

The ICRTF will also stand up projects led by willing members, with Australia providing leadership and support. These projects will be developed to assist members to increase their resilience through knowledge sharing and information exchange.

Australia's leadership in the establishment of the ICRTF underscores the importance of international collaboration in addressing ransomware threats. Through its chairmanship, Australia will foster cooperation, capacity building and help shape the development of global norms, resulting in a more resilient and secure digital environment. The ICRTF serves as a testament to the collective efforts of nations, industry leaders and cyber security experts in the fight against ransomware on a global scale.



Chapter 2: Potential growth opportunities for Australia



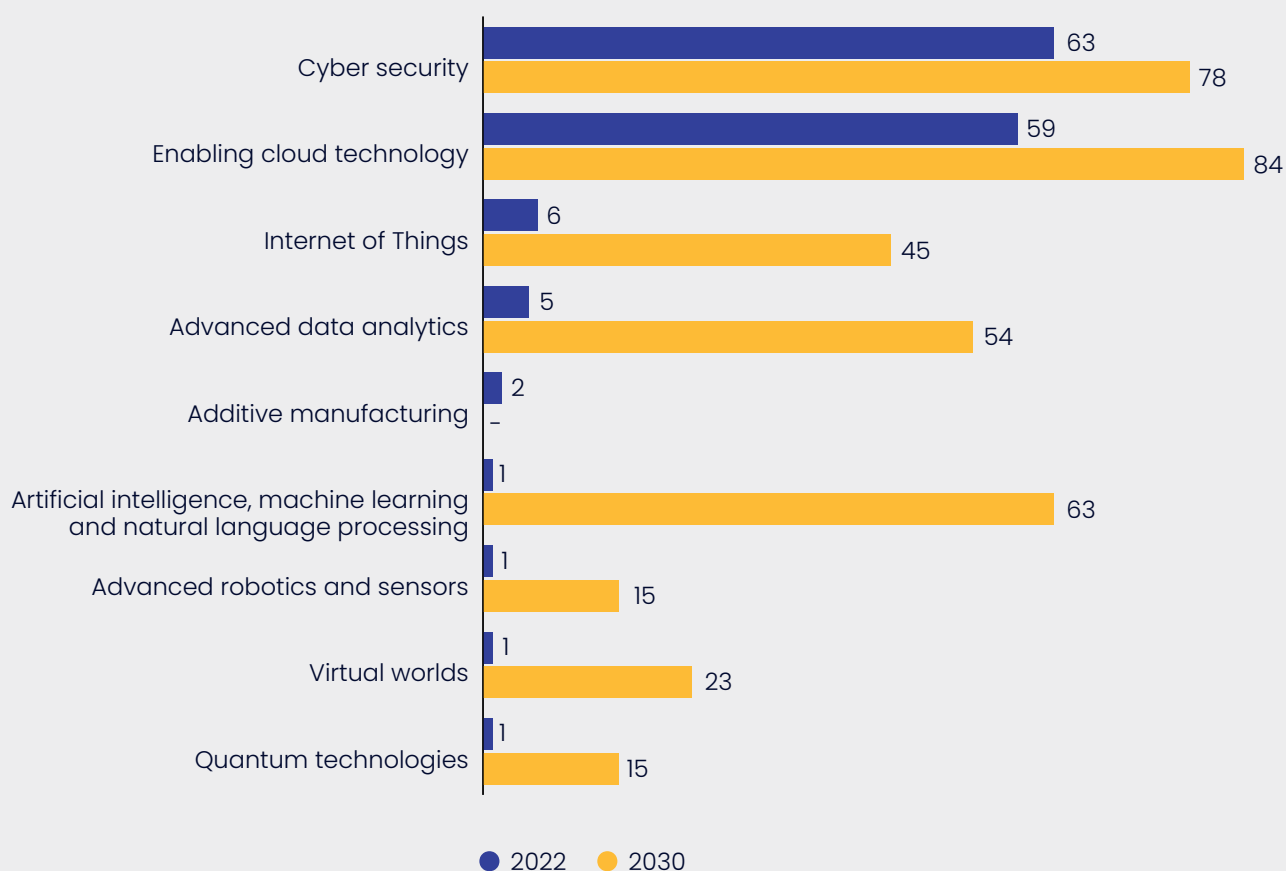
The Australian cyber security sector today

Internationally, Australia currently holds the 19th position³³ in a global ranking of international competitiveness among 64 nations, up from 31st position in 2022. Nevertheless, there is a clear imperative for Australia to embark on a journey of economic diversification, while simultaneously amplifying its focus on entrepreneurship and bolstering cyber security. It is noteworthy that Australia's standings in these two domains are less than optimal, with entrepreneurship ranked 62nd and cyber security placed at 53rd. On a brighter note, Australia continues to be an appealing destination for launching new ventures, boasting commendable rankings in terms of startup procedures and duration, a robust educational system and relatively low exposure to sovereign and political risks³⁴.

Conversely in 2022, Australia was ranked as the world's fifth 'cyber power' with the US, China, Russia and the UK rounding off the top five. Australia ranked significantly high across two of the eight objectives measured – defence and intelligence – demonstrating intent and capability to pursue objectives³⁵.

Over the preceding years, Australian businesses have had high levels of adoption of key digital infrastructure such as cyber security and cloud, but lower adoption of more advanced technologies. The rate of cyber security adoption in Australia is expected to accelerate from 63 percent in 2022 to 78 percent in 2030, a shift attributed to the diversification of business investments across various digital technologies³⁶.

Figure 6. Adoption of critical technologies by Australian businesses (%), 2022 and 2030



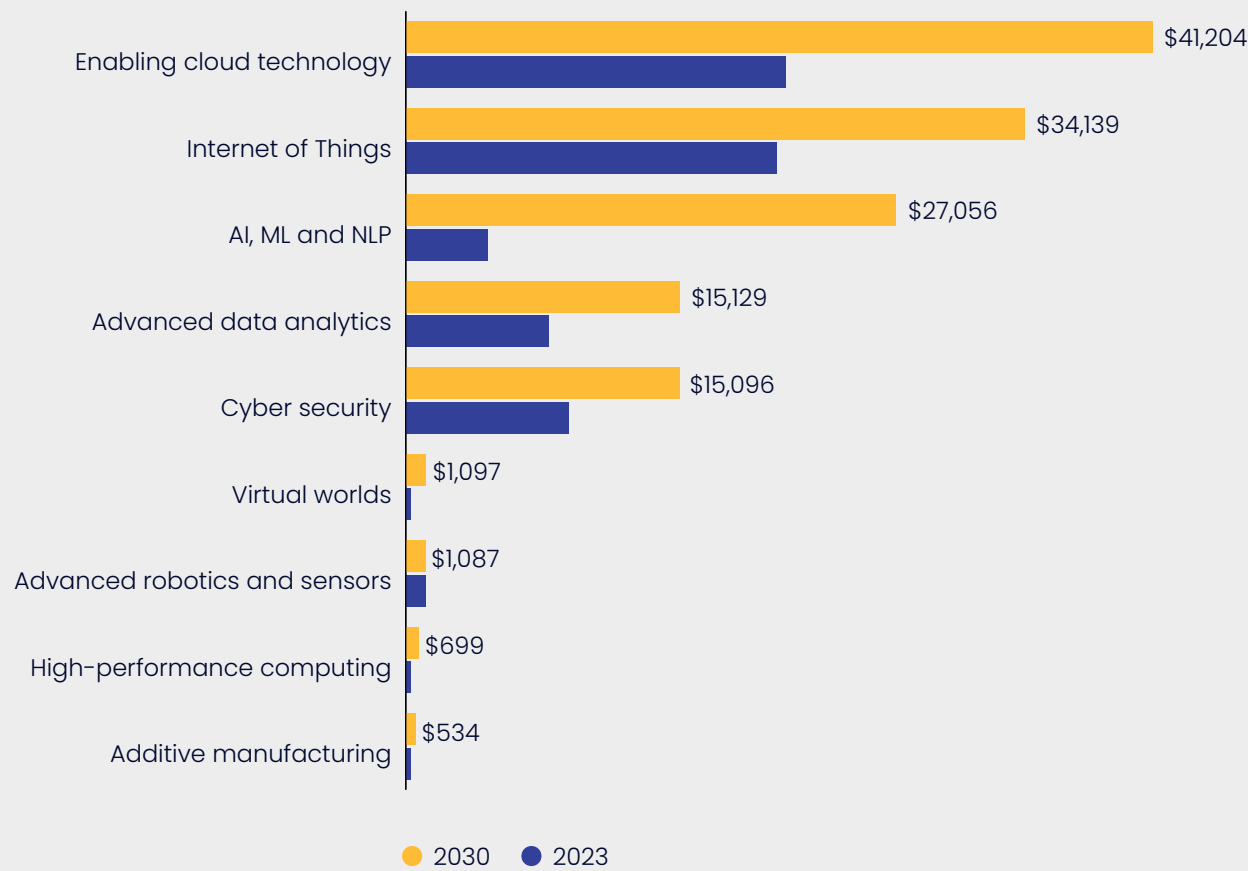
³³ IMD World Competitiveness Yearbook 2023, CEDA

³⁴ IMD World Competitiveness Yearbook 2023, CEDA

³⁵ National Cyber Power Index 2022, Belfer Center for Science and International Affairs

³⁶ Australia's Digital Pulse 2023, ACS

Figure 7. Investment in emerging technologies in 2023 and 2030 (AU\$ million)¹⁹



Australia’s cyber security sector continues to be a vital component of the nation’s economic landscape, primarily due to the escalating digital threats and demand for critical cyber security services. As a sector, cyber security offers Australia a new source of economic growth. It also enables growth through digital transformation in every sector of the economy.



¹⁹ Australia’s Digital Pulse 2023, ACS

As businesses rely on the confidentiality and integrity of digital information, a strong domestic cyber security sector is critical for Australia's competitiveness and international reputation as a trusted place to do business and for the nation's continued economic growth. The value it brings is multifold, with implications across economic, employment and technological arenas:

Increased cyber threats: The growth of the cyber security sector in Australia has been driven by the rising number and sophistication of cyber threats. Cyber attacks, data breaches and ransomware incidents have surged in recent years, with Latitude Financial, Optus and Medibank demonstrating the cascading effect across all sectors of the economy.

Government initiatives: The federal government has been actively involved in bolstering cyber security efforts through the establishment of the National Office of Cyber Security and appointment of a National Cyber Security Coordinator, as well as the release of the 2023–2030 Australian Cyber Security Strategy.

Private sector investment: Significant investments from private sector organisations, including cyber security companies and financial institutions, will continue to fuel the growth of the sector such as the announcement of Microsoft's AU\$5 billion investment to build up its Australian hyper-scale cloud computing and artificial intelligence infrastructure.

Small business sector: Australia's small business sector contributes AU\$500 billion of economic activity, constituting one-third of Australia's GDP³⁷. For a small business, even a minor cyber security incident can have devastating impacts, causing serious financial and reputational damage, with significant flow on effects to the Australian economy.

Skills and workforce development: There is a growing emphasis on developing a skilled cyber security workforce in Australia to meet the demand for cyber security professionals, through initiatives being led by the Future Skills Organisation and reforms to the VET sector. A recent focus on diversity was evident through the Federal Government's Cyber Security Skills Partnership Innovation Fund.

Innovation: Australia is becoming a hub for cyber security innovation and startups. Many startups are developing innovative solutions to address emerging threats with the federal government's R&D Tax Incentive continuing and most states and territories providing startup funding and support.

Legislation and regulation: Federal government continues to legislate positive cyber security obligations and management for business and critical infrastructure providers, influencing the sector's growth by requiring organisations to report data breaches.

International collaboration: Australia has been collaborating with international partners on cyber security initiatives and information sharing to improve its cyber resilience, most notably AUKUS and the continued work undertaken by the Department of Foreign Affairs and Trade's Cyber and Critical Tech Cooperation Program.

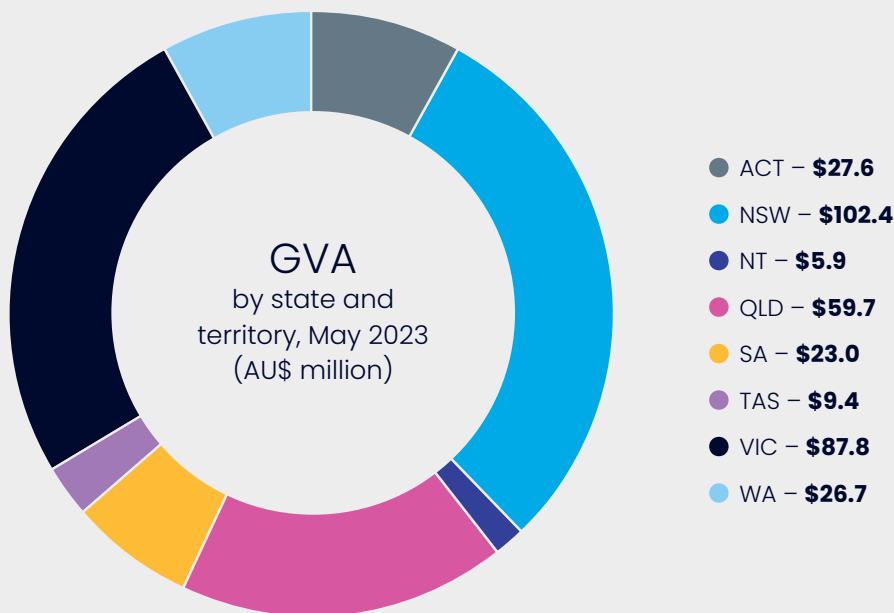
How growth is being achieved

Australia's cyber security sector generated an estimated AU\$3.99 billion of Gross Value Added (GVA) in 2023, up from AU\$2.4 billion in 2022

Analysis from Oxford Economics Australia provides the following key insights for 2023:

- **Gross revenue** of Australia's cyber security sector expanded significantly to AU\$6.9 billion.
- **Average salaries** in the sector were AU\$123,160, with a slight difference seen between the public sector at AU\$119,694 and the private sector at AU\$124,331³⁸.
- **Gross Value Added (GVA)** is noteworthy at AU\$3.99 billion, making it comparable to other digital sectors.

Figure 8. GVA by state and territory, May 2023 (AU\$ million)



38 The \$123k figure is a weighted average reflecting the higher proportion of cyber security specialists working in the private sector

There are over 315 cyber security firms in Australia, with 83 percent located in eastern states

There has been no significant decline in the number of businesses providing cyber security products and services operating in Australia. By December 2023, Australia was home to over 315 cyber security businesses, demonstrating the resilience of this sector post the COVID-lockdown period. The average age of a cyber security company in 2023 was 5.5 years, compared to 4.8 years in 2022³⁹.

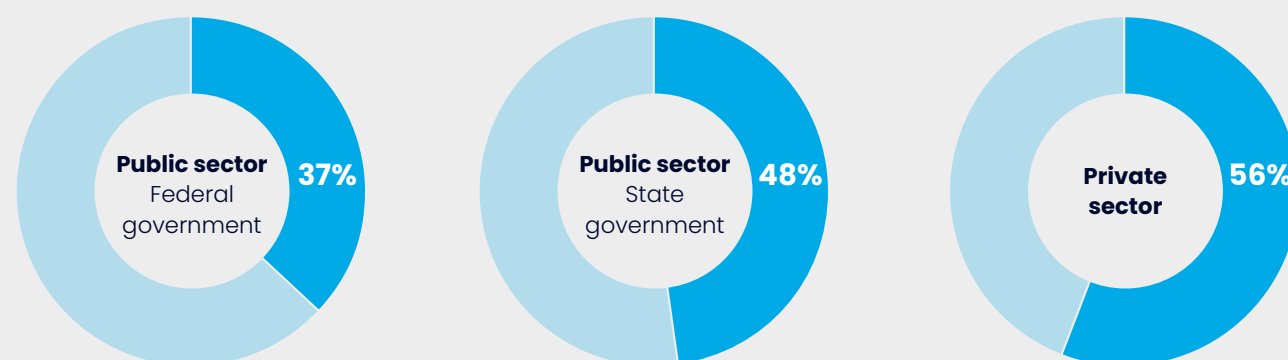
Figure 9. National company composition data (%)

Size⁴⁰

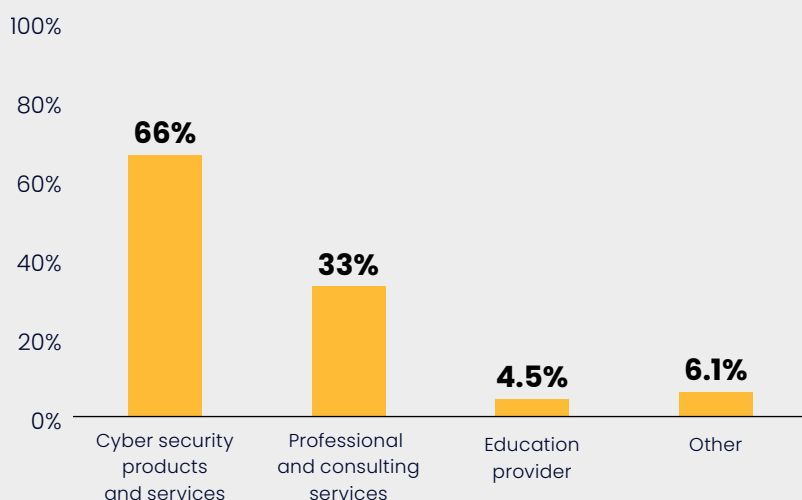


Client⁴¹

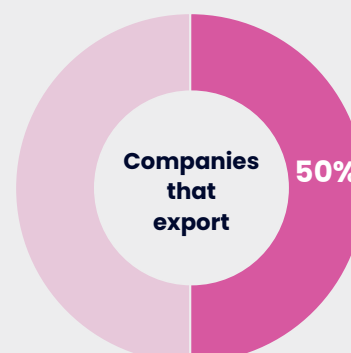
Percentage of companies serving the:



Business focus area⁴²



Export⁴³



39 AUCyberscape as at 31 December 2023
 40 AUCyberscape as at 31 December 2023
 41 2023 Australian Cyber Security Sector Survey, AustCyber
 42 AUCyberscape as at 31 December 2023
 43 2023 Australian Cyber Security Sector Survey, AustCyber

Figure 10. HQ locations and average ages of cyber security companies by state and territory



Number of company headquarters

in state/territory in 2023⁴⁴



Average age of companies

in state/territory in 2023⁴⁵

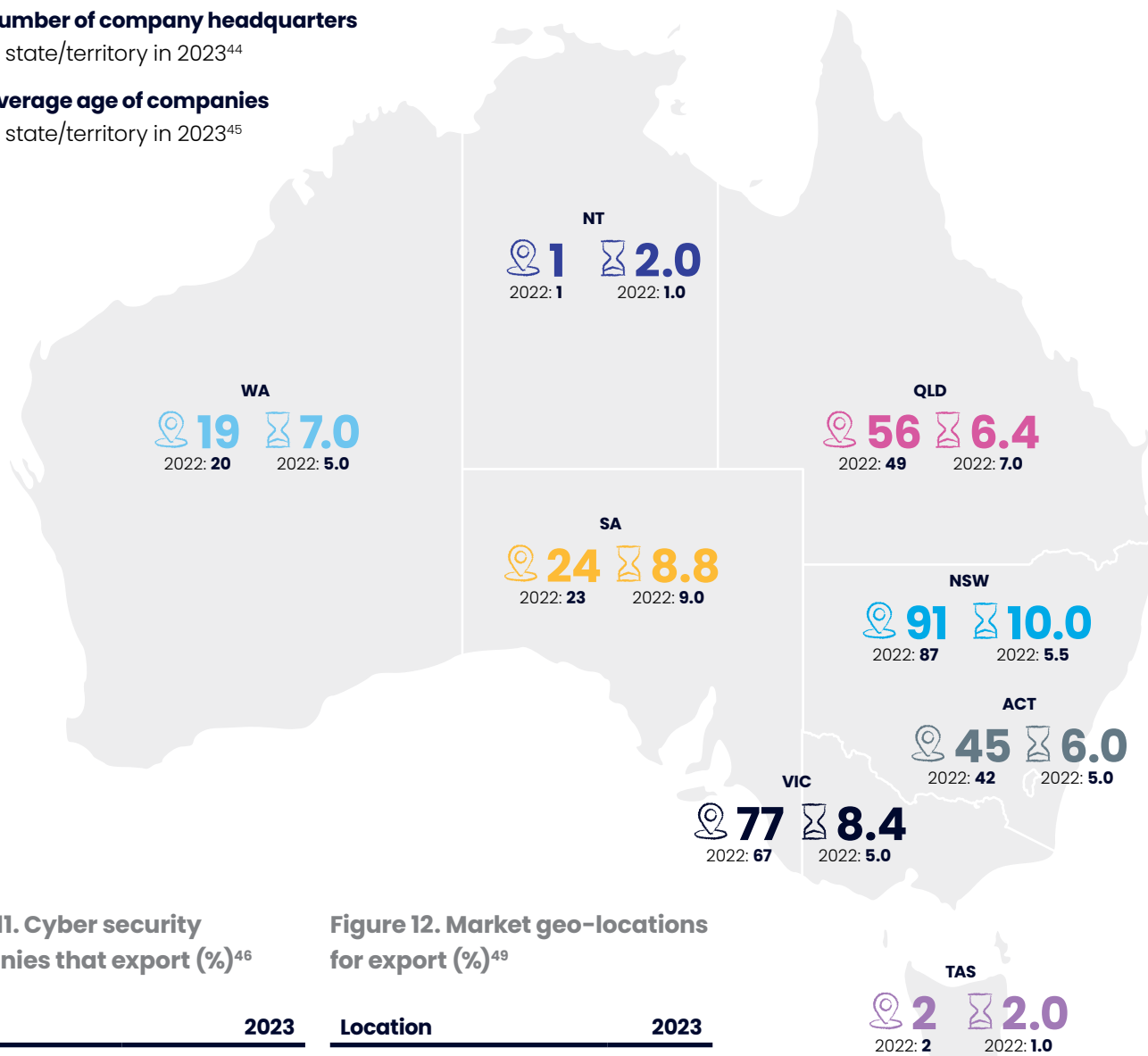


Figure 11. Cyber security companies that export (%)⁴⁶

State	2023
ACT	80%
NSW	40%
NT	NA ⁴⁷
QLD	50%
SA	20%
TAS	NA ⁴⁸
VIC	53%
WA	50%

Figure 12. Market geo-locations for export (%)⁴⁹

Location	2023
Americas	20%
ASEAN	39%
Europe	26%
Middle East & Africa	21%

⁴⁴ 2023 Australian Cyber Security Sector Survey, AustCyber

⁴⁵ AUCyberscape as at 31 December 2023

⁴⁶ 2023 Australian Cyber Security Sector Survey, AustCyber

⁴⁷ No data provided by any NT cyber security companies

⁴⁸ No data provided by any Tasmanian cyber security companies

⁴⁹ AUCyberScape as at 31 December 2023

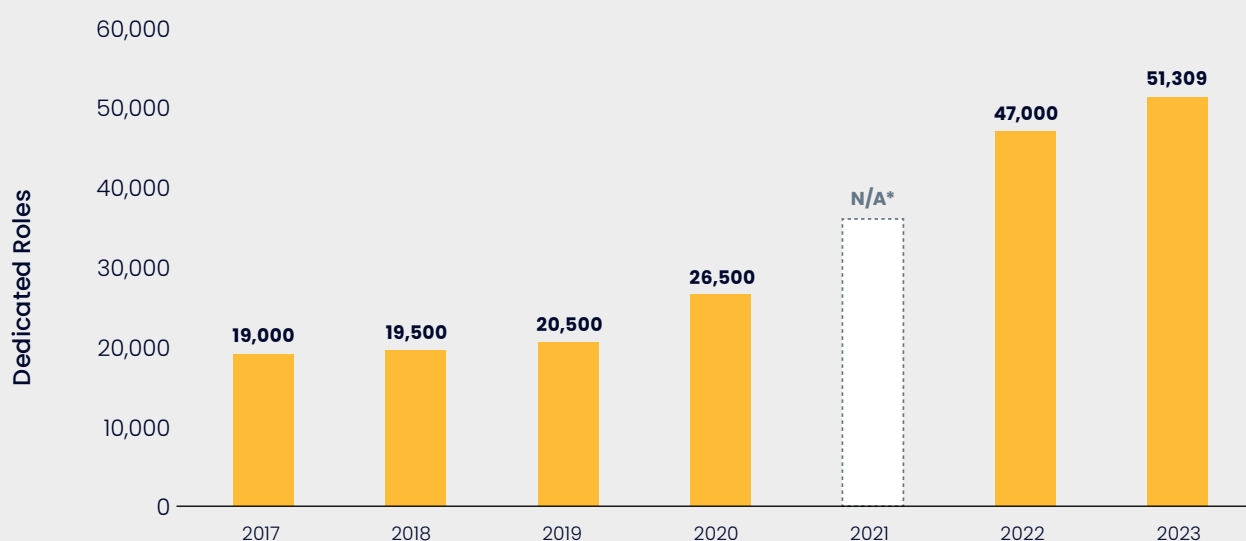
The demand for cyber security professionals continues to widen the skilled workforce gap

Analysis from Oxford Economics Australia provides the following key insights for 2023:

- A total of 125,791 people were employed in the cyber security sector⁵⁰.
- 51,309 were identified as Dedicated Roles (41%), an estimated increase of 9.5 percent since the previous year.
- 74,482 were identified as Related Roles (59%) requiring cyber skills knowledge⁵¹.
- Of the Dedicated Roles, 24,254 were identified as Core Roles, requiring technical expertise (19%).
- Women hold 17 percent of cyber security Roles⁵².
- By 2030, it is projected that an additional 33,691 Dedicated Roles will be needed to meet the demand⁵³.
- The average salary for a cyber security role is estimated at AU\$123,160, with those employed in the public sector receiving a marginally lower salary of AU\$119,694, compared to private sector counterparts at AU\$124,331.
- Since 2019, enrolments in security science degrees have increased by 30 percent per annum⁵⁴.

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 roles, as well as indirect roles, as it underpins the digitisation and growth of the entire economy. Cyber security architects are the most in demand cyber security role, followed by engineers and analysts when comparing several leading recruitment platforms.

Figure 13. Cyber security workforce (Dedicated Roles) 2017–2023 (n.)⁵⁵



*The Sector Competitiveness Plan was not produced in 2021

⁵⁰ AUCyberExplorer

⁵¹ ABS Census Data 2021

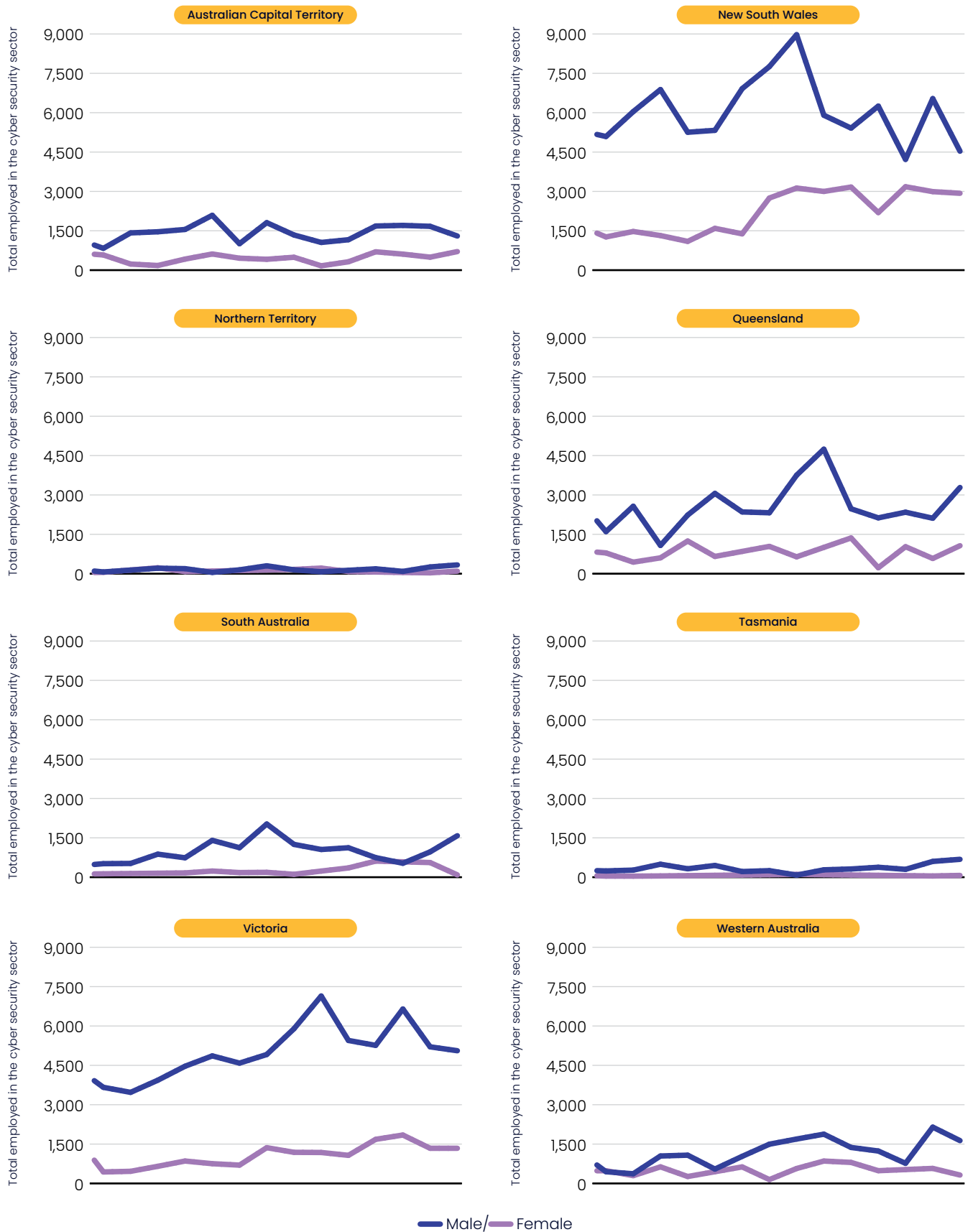
⁵² Gender Dimensions of the Australian Cyber Security Sector Report 2023, RMIT and AWSN

⁵³ Oxford Economics Australia analysis

⁵⁴ Based on the Australian Standard Classification of Education (ASCED) code 029901. This code is focused only on security science related to information technology. Given its relatively limited scope, it is not likely to capture all the enrolments in the sector, so this growth number should be considered as a lower bound estimate.

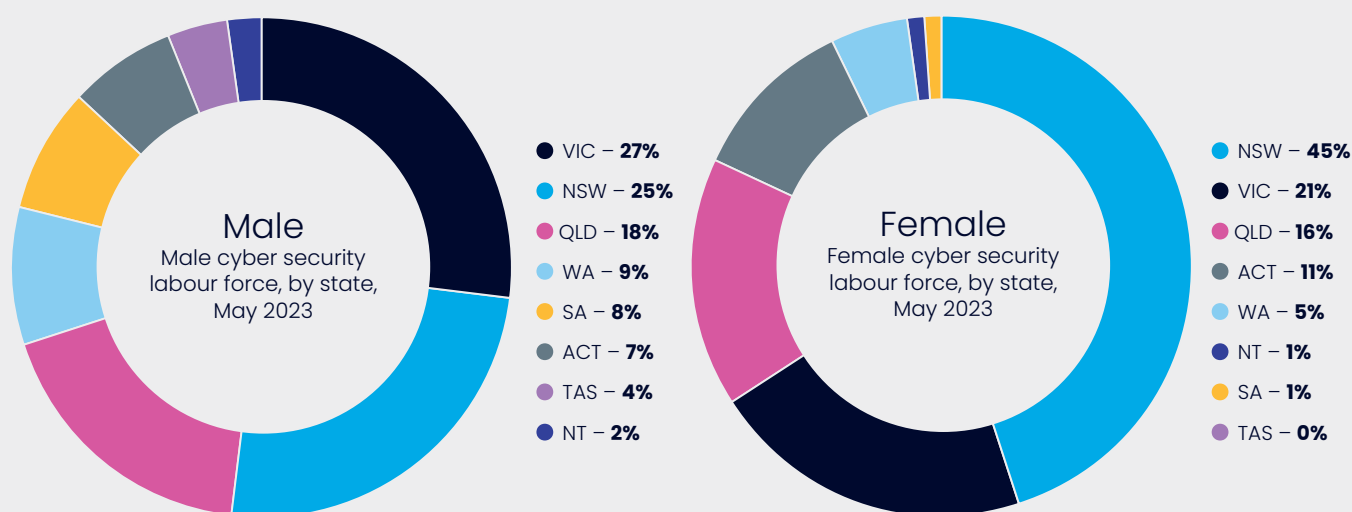
⁵⁵ Sector Competitiveness Plans 2017–2023, AustCyber

Figure 14. Cyber security workforce by state and gender 2020–2023⁵⁶



⁵⁶ Oxford Economics Australia

Figure 15. Cyber security company staff profile by state and territory (%)^{57,58}



	ACT	NSW	NT	QLD	SA	TAS	VIC	WA
Technical	63	61	67	63	62	50	72	74
Non-Technical	37	39	33	37	38	50	28	26

The frequency and severity of cybercrime has risen⁵⁹

In 2022–2023, Australia experienced an estimated 94,000 cybercrime reports (one every 6 minutes), an increase of 23 percent compared to the previous financial year. However, it should be noted that globally, cybercrime has reduced by 14.5 percent since reaching a global peak in 2021.

The Australian Signals Directorate responded to over 1,100 cyber security incidents in 2022–2023, with 10 percent of all incidents identified as ransomware – this was comparable to the previous year. Of these, 143 incidents related to critical infrastructure.

Average cost of cybercrime per incident reported, up 14 percent:

- small business: AU\$46,000
- medium business: AU\$97,200
- large business: AU\$71,600

Nearly 94,000 cybercrime incident reports, up 23 percent:

- on average 1 report every 6 minutes
- an increase from 1 report every 7 minutes

Top three cybercrime types for individuals:

- identity fraud
- online banking fraud
- online shopping fraud

Top three cybercrime types for business:

- email compromise
- business email compromise (BEC) fraud
- online banking fraud

⁵⁷ AUCyberscape as at 13 December 2023

⁵⁸ Oxford Economics Australia

⁵⁹ Australian Signals Directorate Cyber Threat Report 2022–2023

Data breaches in 2023 focused on the financial and healthcare sectors, with several high profile, high impact breaches occurring to Latitude Financial, Optus, HWL Ebsworth and Medibank.

The first Australian Institute of Criminology Report through the Cybercrime in Australia series was published in 2023, and aimed to provide a clearer picture of cybercrime victimisation, help-seeking and harms among Australian computer users.



Cybercrime victims are not evenly distributed, with certain sections of the community more likely to be a victim.

18 – 24-year-olds (38.9%) were more likely to be cybercrime victims than 65 years and above (22.7%).

- **Men** were more likely than **women** to be the victim of fraud and scams (9.1% vs 6.4%).
- **First Nations Australians** were more likely than **non-Indigenous respondents** to become victims of malware (41.6% vs 21.1%) and identity crime (41.0% vs 19.4%) and four times as likely to become the victim of fraud or scams (28.6% vs 7.0%).
- **Respondents who identified as LGB+** were more likely than heterosexual respondents to have been a victim of malware (24.8% vs 21.6%).
- Respondents who mainly **spoke another language** other than English at home were more likely to have been a victim of malware (28.1% vs 21.5%), identity crime and misuse (25.6% vs 19.8%) and scams and fraud (12.6% vs 7.5%)⁶⁰.

⁶⁰ Australian Institute of Criminology Cybercrime in Australia 2023

The report highlighted that some of these differences may be due to online behaviour and technology use; frequent social media use. The longer time spent for personal use online, the more likely they were to be a victim of cybercrime.

Far-reaching impacts of the HWL Ebsworth Data Breach

Organisations across the world face an ever-increasing risk of cyber threats and data breaches. The legal industry has not been immune to these challenges. This case study examines the data breach incident at HWL Ebsworth, a prominent Australian law firm, with high profile ASX listed companies as well as federal and state governments.

HWL Ebsworth is one of Australia's largest and most well-established law firms, providing legal services to a diverse client base – including corporations, government agencies and individuals. The firm manages sensitive and confidential information critical to its clients' legal matters, making data security paramount to its operations.

In 2023, HWL Ebsworth suffered a significant data breach which involved unauthorised access to its client database and confidential legal documents. The breach was discovered when unusual network activity was detected, prompting immediate investigation. The breach was traced back to a cyber attack that exploited vulnerabilities in the firm's IT infrastructure.

The data breach had far-reaching implications for HWL Ebsworth's supply chain, affecting multiple stakeholders:

- 1. Client trust:** The breach eroded the trust of HWL Ebsworth's clients, who relied on the firm to safeguard their sensitive legal information. Many clients reconsidered their relationship with the firm, impacting revenue and long-term business relationships.
- 2. Reputation damage:** The incident garnered significant media attention and public scrutiny. The negative publicity damaged the firm's reputation, making it harder to attract new clients and retain existing ones.
- 3. Legal liability:** HWL Ebsworth faced legal liability for failing to protect client data adequately. Lawsuits and regulatory fines added financial strain to the firm's operations.
- 4. Third-party impact:** The breach also affected third-party vendors and partners who collaborated with the law firm. These organisations had to assess their own cyber security vulnerabilities and consider potential impacts on their business relationships with HWL Ebsworth.

The HWL Ebsworth data breach serves as a stark reminder of the severe consequences that a cyber security incident can have on an organisation's supply chain. It underscores the importance of proactive cyber security measures, effective incident response and maintaining the trust of clients and stakeholders in mitigating the potential fallout from such incidents. As data breaches are a constant threat, organisations must remain vigilant and prioritise cyber security to protect their operations and supply chains.

Federal government strengthens cyber security policies, strategies and frameworks

The importance of continued investment and support in cyber security cannot be overstated. Recognising the ever-evolving cyber threats faced by individuals, businesses and the nation at large, the federal government has taken significant strides to fortify the nation's cyber defences. From substantial budget allocations to policy frameworks, the federal government has continued to underscore the recognition of cyber security as a vital component of national security and economic resilience.

2023 saw several new announcements by the federal government and continued implementation for investment and support to the cyber security sector:

- **National Office of Cyber Security** (AU\$37.3 million/4 years) to coordinate its cyber security efforts and respond to incidents.
- **National Skills Agreement** (Fee-Free TAFE) (AU\$1 billion*/1yr) to address skill shortages in high priority areas.
- **2023–2030 Australian Cyber Security Strategy** (AU\$586.9 million/7 years) to realise the Australian Government's vision of becoming a world leader in cyber security by 2030.
- Announced in 2022, the **Cyber Skills Partnership Innovation Fund Round 2** (AU\$25.4 million) commenced implementation with the aim of increasing the diversity of the cyber security workforce, with a specific focus on women and First Nations Australians.




* inclusive of state and territory matched funding

Through the AustCyber Projects Fund (a AU\$15 million, three-year initiative designed to help the Australian cyber security industry grow and take ideas global), a significant investment of AU\$335,432[†] was allocated in its third and final round. The funding was strategically allocated to pioneering organisations that are actively shaping the future of cyber security.

[†] there is still one project to be completed by 30 June 2024



Figure 16. AustCyber Projects Fund allocation 2023 (AU\$)

Organisation	Project name	Outcome	2023 Funding
 Penten Pty Ltd (ACT)	HoneyTrace	<p>The global introduction of a cyber security SaaS platform, HoneyTrace.</p> <p>This project focused on launching HoneyTrace worldwide and encompassed various stages – including producing productisation documentation, developing marketing materials, establishing the product website at honeytrace.io, conducting user trials and hosting a launch event.</p>	\$95,352
 Cynch Security (VIC)	Cyber risk assurance for small critical infrastructure suppliers	<p>The design of the Cynch Cyber Fitness platform focused on small businesses, offering them a simple means to enhance their cyber resilience.</p> <p>Collaborating with major enterprises like Telstra, Cynch developed a supply chain assurance solution that prioritised the needs of small businesses and their collaborators. This solution assists them in meeting their responsibilities.</p>	\$205,080
 Forticode	Forticode (VIC)	CipherToken	\$35,000

CYBERMERC ›

Cybermerc: Sovereign innovation supported through government initiatives

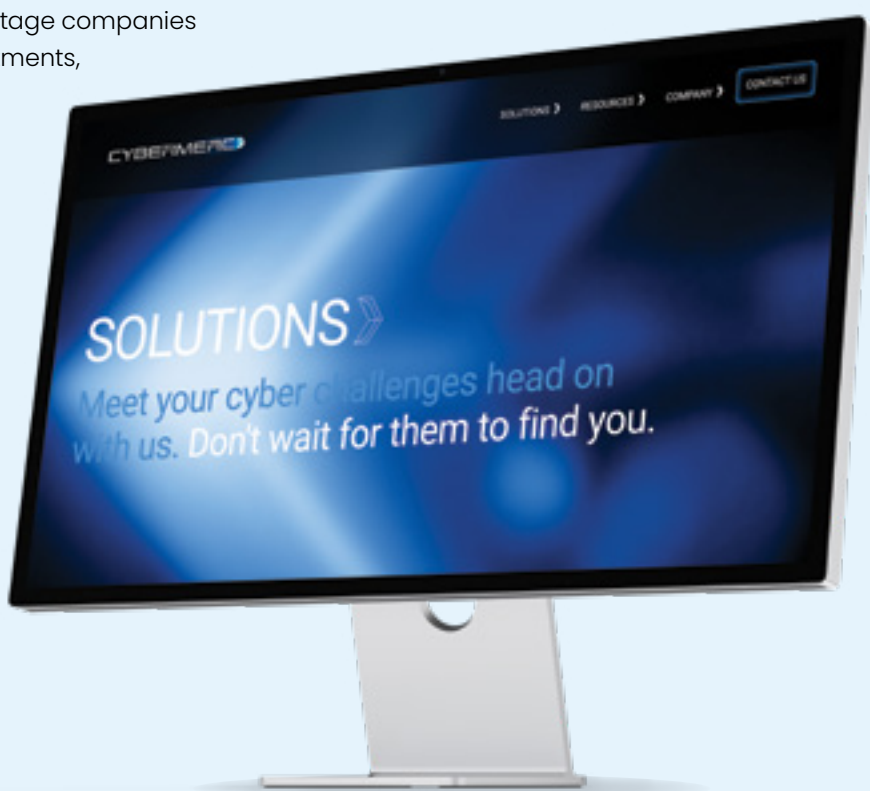
As an Australian cyber security company founded in 2016, Cybermerc provides national threat intelligence sharing capabilities and cyber security education and training services to the private and public sectors. The company was founded by brothers Matthew and Paul Nevin who recognised the need for improved cyber threat intelligence sharing and education and training in their prior careers in government.

In its early years, Cybermerc was a recipient of 'seed funding' from the AustCyber Projects Fund. Matthew credits this funding as being instrumental to the company's success. Unlike private investment, AustCyber's funding did not require relinquishing shares or implementing an exit strategy. Instead, it allowed them to focus on building a sovereign capability and achieving strategic outcomes, rather than short-term growth and profits.

Cybermerc was able to develop its flagship product, AUSHIELD DEFEND, a threat intelligence platform that connects government agencies and businesses together. Multiple federal government agencies and private sector companies now use AUSHIELD. The funding also supported the development of Cybermerc's cyber range, a pivotal training component for real-world practical training and education programs.

Cybermerc notes that a lack of early-stage investment remains a challenge for sovereign Australian cyber security companies. Without programs like the AustCyber Projects Fund, companies struggle to get off the ground. Cybermerc expressed concerns that without addressing the cyber investment gap, Australia risks losing its ability to develop sovereign cyber capabilities internally. They argue that the government needs to support early-stage companies through appropriate risk-taking investments, as other nations like Israel and the US do to foster competitive homegrown industries. This is particularly critical for sovereign national security related capabilities.

Cybermerc's story shows the impact that targeted government funding can have in nurturing strategic national capabilities.



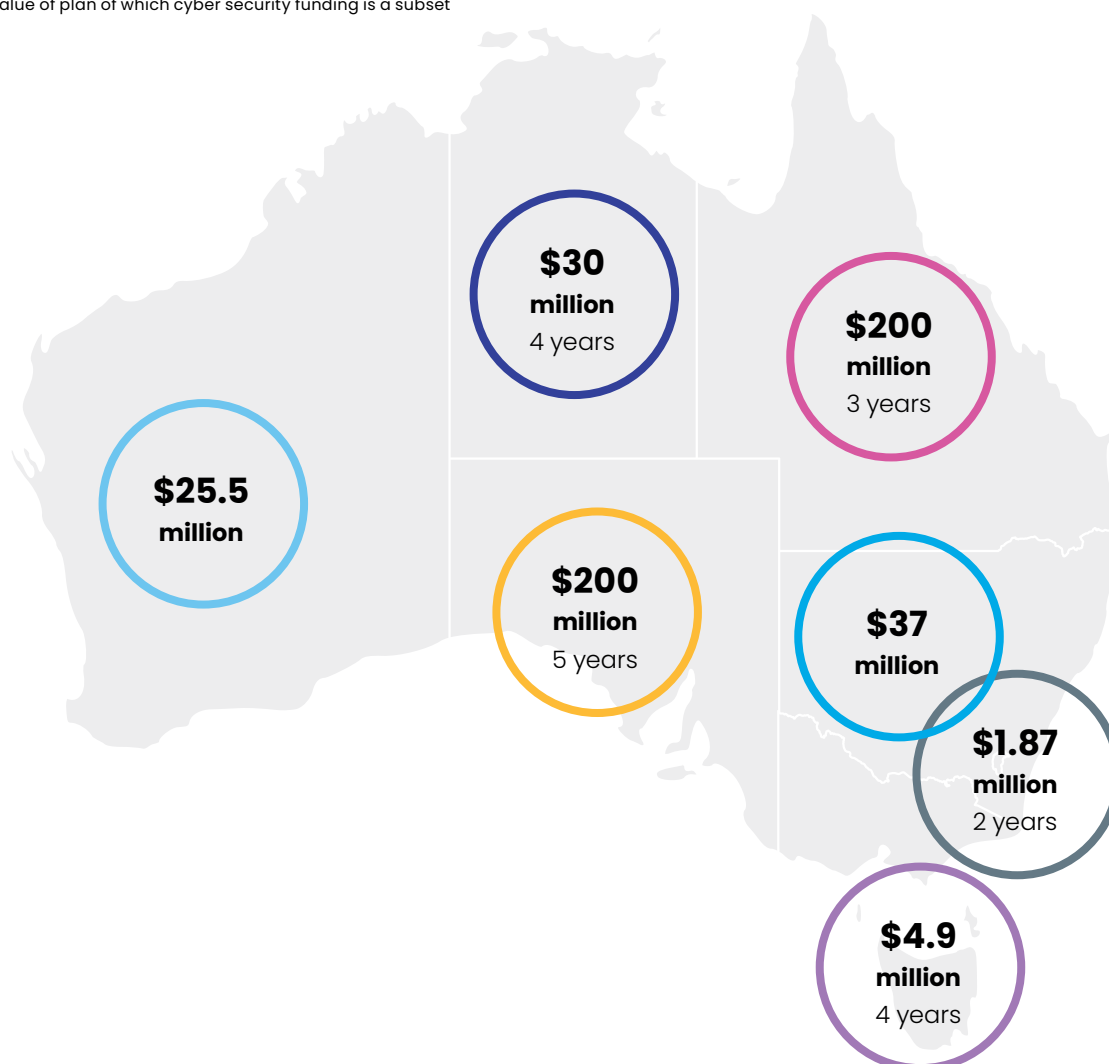
States and territories are developing their own communities to foster innovation

Australian states and territories have demonstrated strong collaboration, with each respective cyber hub or government department responsible for cyber sector development connecting on a regular basis to share ideas, programs and initiatives to grow the sector and help close the cyber skills gap.

Australian states and territories also continue to focus on creating uplift in government digital services and increasing cyber security measures, committing to matched funding under the National Skills Agreement, with additional announcements for investment and support in 2023:

State	Program	Investment (AU\$)
ACT	Canberra Cyber Hub	\$1.87 million/2yrs
NSW	Digital Restart Fund	\$37 million*
NT	Enhance cyber security controls and capability	\$30 million/4yrs
QLD	Digital Economy Strategy	\$200 million/3yrs*
SA	Digital Investment Fund	\$200 million/5yrs
TAS	Whole of Government Cyber Security Program	\$4.9 million/4yrs
WA	Digital Capability Fund	\$25.5 million

*whole value of plan of which cyber security funding is a subset





Cyrise: A model formula for accelerating, supporting and investing in world-class cyber security solutions

As Australia's first dedicated cyber security incubator, CyRise was launched in 2017. It was born out of a partnership between Dimension Data (now NTT) and Deakin University, with funding support from the Victorian Government's LaunchVic initiative. It has been pivotal in shaping the Australian cyber security ecosystem. However, after five years of successful collaboration, the program came to its natural conclusion on 19 May 2023.

Reflecting back, investing in Australian cyber security startups through the CyRise program has proven to be a valuable venture. The incubator supported 39 startups, with many raising additional capital following their participation in the program. At least 12 of the companies raised over a million dollars, and two of those secured more than AU\$10 million dollars, with both local and international investors. The cohorts have developed world leading technology; and clients include federal and state governments, banks and private practice.

CyRise's success can be attributed to several factors:

- **Joint venture structure** – CyRise operated as a collaboration between a university and an IT service provider, so they were able to offer both academic and practical insights into cyber security challenges.
- **Quality deal flow** – the accelerator focused on curated and quality-driven deal flow, ensuring that promising startups and innovative solutions were at the forefront of their activities.
- **Skilled mentoring** – CyRise provided its participating companies with skilled mentors who played a pivotal role in shaping their learning, networking and development. This mentorship enhanced the 'know-what', 'know-how,' and crucially the 'know-who' for entrepreneurs.
- **Innovation and networking** – CyRise encouraged innovation and building robust networks. Such networks enable startups to connect with industry leaders, potential investors and other beneficial partners.
- **Collaboration** – the accelerator promoted collaboration within the ecosystem, ensuring that startups worked together, shared insights and benefited from shared experiences.

These offerings and practices enabled CyRise to stand out as a successful accelerator in Australia. The combination of high returns and the potential for sustained growth makes CyRise startups a prime choice for forward-thinking investors.



Chapter 3: Challenges to sector growth



In 2023, Australia's cyber security outlook stood on a precipice – with high-profile data breaches, including state-sponsored cyber attacks, economic impact to businesses due to cyber attacks, geo-political tensions and economic trade sanctions. This was further marred by the release of new, untested, unregulated technologies, software and applications.

With a somewhat simple, yet factual outlook to 2023, Australia's security sector emerges with positive growth against this backdrop; GDP, GVA, workforce and investments by public and private sectors increased Australia's resilience to these threats. However, there is more that needs to be done to bolster Australia's competitiveness in the global market and build upon the economic value cyber security brings nationally.

This Sector Competitiveness Plan identifies four key barriers for growth relative to international peers. To remain globally competitive, Australia must improve its support for:

1. cyber security startups and the commercialisation of their sovereign technology;
2. domestic procurement of cyber security products and services;
3. public-private partnerships to attract and upskill cyber security talent; and
4. attracting investment into a rapidly maturing industry.

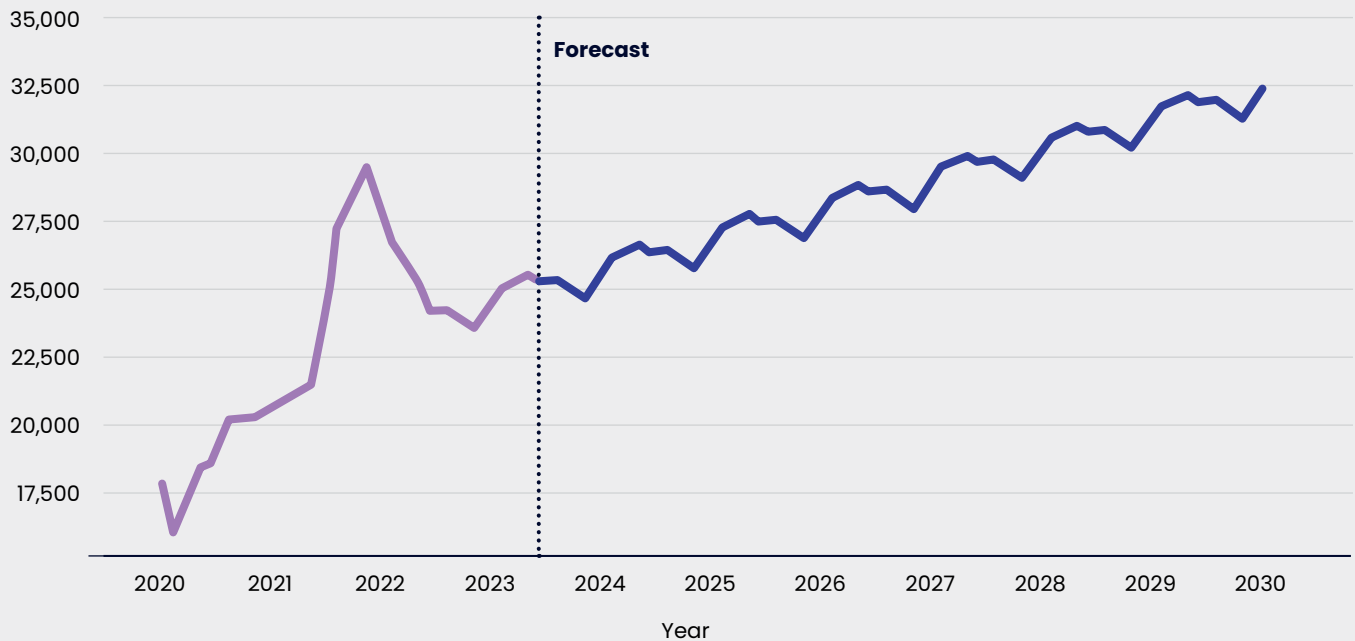


The Australian cyber security sector GVA could contribute an additional 32 percent to the Australian economy by 2030

The cyber security sector has an opportunity to increase the national GVA to AU\$5.2 billion by 2030, an increase of AU\$1.26 billion from 2023.

The projection has been developed by grouping the monthly GVA forecasting into financial year (FY) terms. The figure of AU\$5.2 billion is the expected GVA in the financial year of 2030, or the result of adding all the monthly estimates from July 2029 to June 2030. The forecasting was developed on the national level GVA calculations for the sector from January 2015 to May 2023, following a random walk model equivalent to a seasonal ARIMA with a drift/trend component.

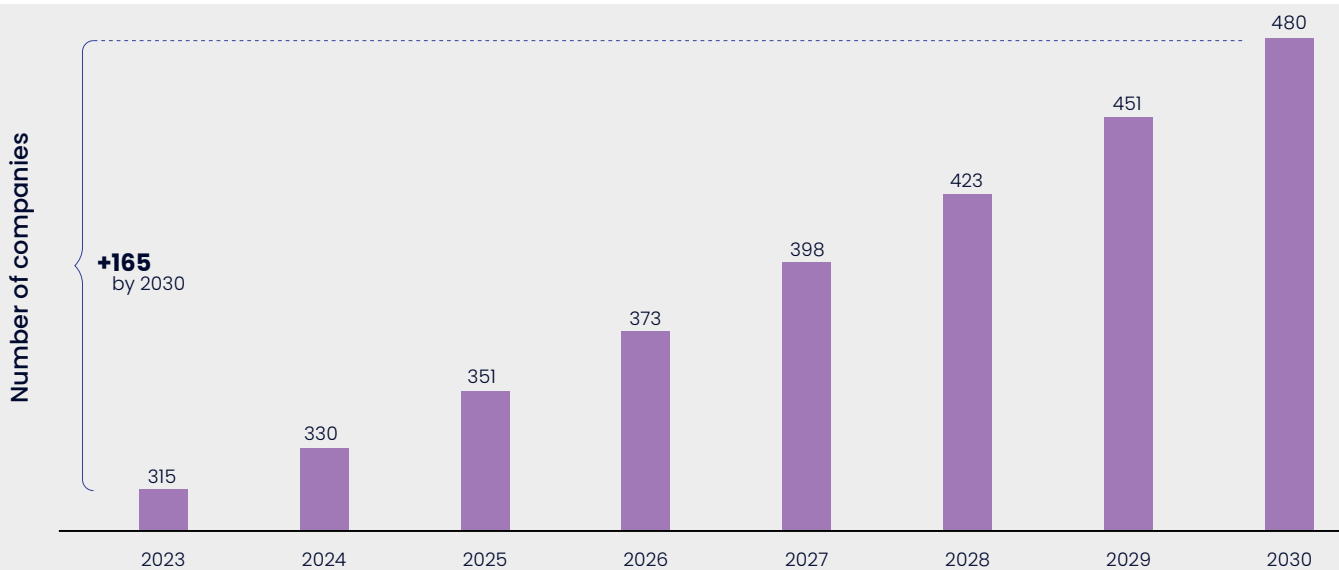
Figure 17. Actual and forecasted GVA in the cyber security sector monthly (AU\$ billion)⁶¹



The Australian cyber security sector could be home to approximately 500 sovereign companies by 2030⁶²

Based on conservative view of historical growth, the cyber security sector could foster an increase of close to 200 homegrown cyber security companies by 2030.

Figure 18. Growth of cyber security companies in Australia (n.)⁶³



⁶¹ Oxford Economics Australia

⁶² AUCyberscape analysis

⁶³ Calculated at an average annual increase of 8 percent on data derived from AUCyberscape

In addition to the committed funding of the 2023–2030 Australian Cyber Security Strategy, the establishment of key programs such as the AU\$15 billion National Reconstruction Fund and the implementation of initiatives such as the Industry Growth Program, will continue to assist in growing sovereign cyber security companies.

Investment companies such as Blackbird Ventures and AirTree stated that technology was the key focus for investment in 2023, with AirTree going as far as highlighting cyber security as a particular interest⁶⁴. However, due to Australia's small venture market compared to international peers, Australian cyber security companies seeking pre-seed, seed or Series A funding look to global markets. Government supported ventures, such as Main Sequence (founded by CSIRO in 2017 to address the 'valley of death' between research and commercialisation) have demonstrated a sustainable and viable model for venture capital. During 2023, Main Sequence Fund 3 raised AU\$450 million, surpassing AU\$1 billion in total funds under management and making its first five Fund 3 investments.

Many government departments and agencies have implemented 'buy Australian' policies, including the federal government's Buy Australian Plan, which aims to support industry sectors through the government's purchasing power. However, the need for initiatives to support procurement of Australian cyber security products and services emerged as a key theme from responses in the 2023 Australian Cyber Security Sector Survey.

The majority of respondents to our survey rated procurement of Australian cyber security products and services as 'poor' (36.3%) or 'fair' (35.2%). Only 4.4 percent of respondents rated procurement as 'very good' and only 1.1 percent rated procurement as 'excellent'.

The Australian cyber security sector will need a potential skilled workforce of 85,000 Dedicated Roles in 2030

This is an estimated 60 percent increase on the 2023 workforce of 51,309, requiring close to 4,813 new hires each year for seven years.

In Australia, there were more than 12,500 unfilled Dedicated cyber security jobs in 2023⁶⁵. In fact, the labour shortage in the global sector keeps growing – with the gap now twice as strong as the workforce⁶⁶.

The 2023 Skills Priority List from Jobs and Skills Australia shows cyber security roles to be some of the highest ranked skills with a national shortage. In addition, with the exception of cyber security engineers, all are identified as having an increased future demand.

64 SmartCompany, Jan 2023

65 Oxford Economics Australia analysis

66 ISC2 2022 Cybersecurity Workforce Study report



Figure 19. 2023 skills priority list shortage⁶⁷

ANZSCO Occupation future demand	National	NSW	VIC	QLD	SA	WA	TAS	NT	ACT
262114 Cyber Governance Risk and Compliance Specialist ⬆	S	S	S	S	S	S	S	S	S
262115 Cyber Security Advice and Assessment Specialist ⬆	S	S	S	S	S	S	S	S	S
262116 Cyber Security Analyst ⬆	S	S	S	S	S	S	S	S	S
262117 Cyber Security Architect ⬆	S	S	S	S	S	S	S	S	S
261315 Cyber Security Engineer ⬇	S	S	S	S	S	S	S	S	S
262118 Cyber Security Operations Coordinator ⬆	S	S	S	S	S	S	S	S	S

⬆ Above economy-wide average ⬇ At economy-wide average S = Shortage

A call for better education and training pathways was a key theme in the 2023 Australian Cyber Security Sector Survey, with 74.3 percent of respondents stating there is a significant skills gap in the industry currently.

Approximately a third to half of all respondents believe there is a need for more skilled professionals in the following disciplines:

- Data security and privacy (53.9%);
- Cloud and software security (47.7%);
- Governance, risk and compliance (43.1%);
- Threat intelligence and security operations (40.0%);
- Incident response and digital forensics (38.5%); and
- Infrastructure security (36.9%).

Respondents also reported a need for more skilled professionals in areas such as marketing and communications, operational technology security, risk management, and security culture and awareness.

⁶⁷ Screen grab taken from the skills priority list at <https://www.jobsandskills.gov.au/skills-priority-list>. S indicates a shortage. The blue upward arrow indicates the skills categories future demand is expected to increase

The challenge for the Australian cyber security sector is more than a skills gap. It is a challenge relating to the rapidly evolving technology landscape. At its core, the rapid evolution of cyber threats demands a workforce that is not only technically proficient, but also continuously updated with the latest in cyber threat intelligence and mitigation techniques. However, there is a rising need for professionals across many other disciplines to understand cyber security concepts and principles as the industry grows. These include law, risk management, criminal justice, human resources and policy development.

A concerted effort across public and private sectors is needed to address:

- focused awareness campaigns promoting cyber security as a career and the development of a pipeline and pathway from primary school aged children;
- continued development and delivery of education and training programs for women and First Nations and neurodivergent people that is flexible and supportive; and
- industry participation in the design and delivery of cyber security programs by creating public-private partnerships for skill-building initiatives, such as SECedu. Led by Professor Richard Buckland, SECedu is a leading Australian network of educators and professionals, founded as a partnership between UNSW and Commonwealth Bank⁶⁸.

The Australian cyber security industry is maturing rapidly and will need to attract investors and support innovation to remain competitive

The Australian cyber security sector, while robust and growing, faces challenges in competing on a global stage and ensuring its solutions are globally recognised. The global cyber security landscape has been dominated by long-established players, primarily from countries like the US, UK and Israel. These nations have a history of innovation, substantial investment and have built strong reputations over decades. In comparison, Australia's cyber security sector is relatively young and still establishing its global footprint.

With 237 Australian based active investors, 2023 venture capital funding totalled AU\$166 million across pre-seed, seed, Series C and Venture rounds for 12 Australian cyber security companies, with 50 percent of the lead investors noted as Australian-based. This is a marked decrease on 2022 venture capital funding of AU\$240 million^{69,70}.

Historically, Australian investors have been known to be more risk-averse compared to their international counterparts. This can lead to hesitancy in investing in sectors perceived as 'new' or 'volatile', such as cyber security. This is in contrast to the CyRise case study featured in chapter 2, which demonstrated that investing in cyber security startups was a good return on investment. By May 2023, the gross Internal Rate of Return (IRR) stood at a commendable 52 percent.

⁶⁸ <https://www.sec.edu.au/>

⁶⁹ Crunchbase

⁷⁰ Australian startup funding in review 2022, Techboard



Key factors to improve Australia's cyber security competitiveness:



Private sector investment



Support for startups



Better government regulations and incentives

The need for continued support of innovation of Australian cyber security startups was a key theme in the 2023 Australian Cyber Security Sector Survey.

Only 8.8 percent of respondents rated the current global competitiveness of Australia's cyber security sector as 'highly competitive' while 20.9 percent rated it as 'not competitive'.

Respondents outlined several key factors to improve Australia's competitiveness. These are:

- increased private sector investment in cyber security (4.02/6);
- better support for Australian cyber security startups (3.96/6); and
- stronger government regulations and incentives (3.94/6).

Respondents also identified what type of collaborations or partnerships would have the most significant impact on enhancing global competitiveness. These are:

- partnerships with Australian businesses for better cyber security integration (4.39/6);
- partnerships with government bodies for strategic planning (4/6); and
- collaborations with international standards bodies for alignment with global practices (3.68/6).

Long term, consistent, diversified investment in cyber security research and development is a key action to create a virtuous cycle of innovation in the sector, as well as infrastructure to support the creation and growth of Australian cyber security companies.

Extending relationships beyond organisational boundaries is important. Collaborations between large companies, startups and venture capitalists are invaluable for acquiring and disseminating knowledge in the cyber security domain. This interconnectedness is crucial in a field as dynamic as cyber security, where threats evolve rapidly and solutions need to be both cutting-edge and collaborative.

Organisations such as CISO Lens are a good example of executing on this action. CISO Lens is an information sharing and analysis community for cyber security executives from the largest organisations in Australia and New Zealand.

The 2023 Australian Cyber Security Sector Survey data reveals a clear mandate for prioritising increased private sector investment in cyber security – with a particular focus on Australian capability, better support for startups and stronger governmental regulations and incentives. These facets were considered most critical by industry stakeholders for bolstering Australia's cyber security sector. Interestingly, partnering with multi-national cyber security companies were given lesser importance, illuminating the sector's focus on strengthening domestic capabilities first.



Australia's leading digital research network, Data61, helping their partners across business, government and industry solve real problems every day

CSIRO's Data61 – the data and digital specialist arm of Australia's national science agency – helps partners across business, government and industry to solve real problems every day. This approach encompasses human-centric methods, advanced AI, quantum computing and cutting-edge networking technologies like 6G. Their focus spans current issues and anticipates future challenges in areas such as digital twins, AR/VR/MR and the secure digitalisation of critical infrastructures.

Recent innovative cyber security solutions:

- **Human-centric cyber security** – Data61 emphasises human-centric security, recognising the role of human factors in cyber security. In collaboration with CSIRO's Collaborative Intelligence Future Science Platform, Data61 integrates AI into Security Operation Centres (SOCs) to assist security analysts in reducing alert fatigue. Additionally, they've gamified cyber security education to enhance awareness and response capabilities across organisational levels in collaboration with partners such as the Cyber Security CRC.
- **AI and cyber security** – Data61 employs a dual approach, ensuring AI security, privacy and trustworthiness by preventing AI/ML-related vulnerabilities and developing AI for robust and optimised cyber defence. Innovations include large language models for software and software-supply-chain security and risk assessment, threat hunting, ransomware prevention, threat modelling and cyber defence automation and augmentation, graph neural networks for web domain trustworthiness, AI security and resilience assessment solutions and airlock technologies for secure data utilisation in collaboration with partners such as the Cyber Security CRC. In the era of large ML models with billions of parameters for effective and timely cyber decision-making, Data61 contributes to the foundational research on model compression, ML IP protection, privacy and data unlearnability.
- **Quantum computing and cyber security** – Data61 is exploring quantum computing as both an enabler of new technologies and a potential threat to internet security. Data61's advancements include post-quantum cryptography algorithms to counter quantum threats and the development of quantum AI systems, tested for resilience against cyber-attacks. Data61 builds new ML models for transitional hybrid systems such as 4/5/6G and quantum/classical computing and investigates how quantum technologies can inspire further development in ML and AI.
- **The quantum future in defence and beyond** – Data61's quantum AI technology is poised to enhance the robustness of future military and defence systems, including electronic and cyber warfare. The technology, while initially developed for defence, through the Australian Army Quantum Technology Challenge, has broader applications for any AI-reliant systems. Additionally, with quantum computers on the horizon, Data61's post-quantum cryptography facilitates the transition to secure network infrastructures in the quantum era.

Chapter 4:

Actions to build a more competitive cyber security sector



A globally competitive Australian cyber security sector will ultimately underpin the future success of every industry in the national economy.

A consolidated effort is needed to continue to build on the maturing sector to sustain Australia's competitiveness and strategic advantages in the creation and commercialisation of cyber security products and services.

To build a stronger cyber security ecosystem to meet national and international demands, a collaborative approach is needed for the following actions:

Remove growth hurdles for cyber security startups to increase the commercialisation of sovereign technology

Finding anchor customers

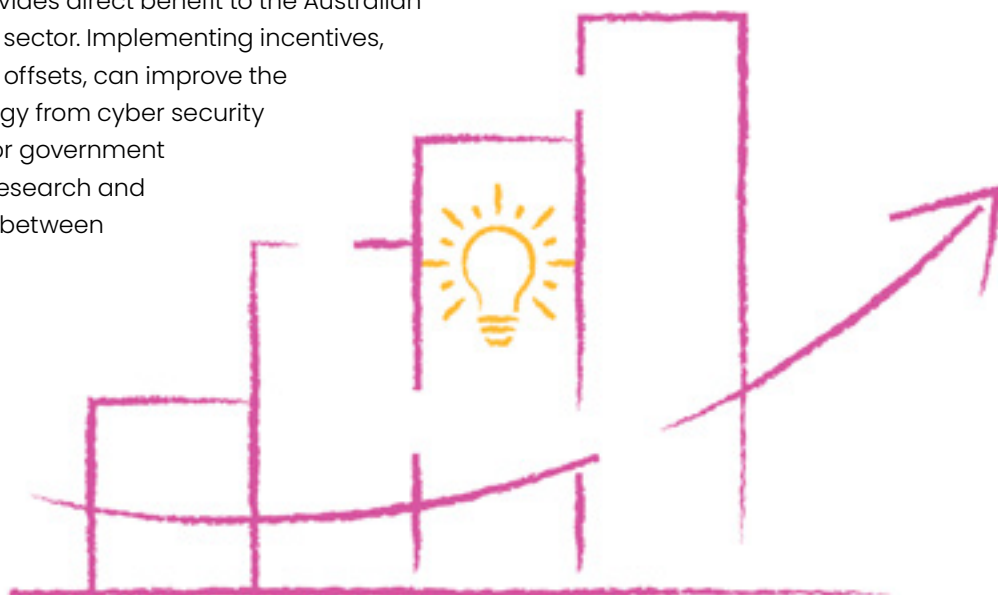
Anchor customers, typically large industry players or government departments, add value to any startup. But for cyber security startups, which rely heavily on trust to gain access to high-risk business areas, anchor customers are one of the most critical ingredients for success as they help establish market legitimacy.

Assisting cyber security startups in their search for customers can help strengthen the competitiveness of the local industry. This is because anchor customers often challenge an emerging company to sharpen its profile and refine its offering to be better aligned with global market needs, which increases business prospects.

Incentives to procure startup technology

Choosing a startup as a vendor for cyber security technology is perceived as risky. There's a lack of stability and unknown longevity; a lean staff profile often equates to poor service, reliability and responsiveness; and it's 'easier' to adopt a solution that is already subscribed to and known in the industry.

However, working with a startup can provide a fresh approach, stimulate innovation and provides direct benefit to the Australian economy and cyber security sector. Implementing incentives, such as tax or other financial offsets, can improve the uptake of sovereign technology from cyber security startups by large enterprise or government departments, and increase research and development collaborations between industry and academia.



Trusted business advisory services

Founders of cyber security startups and small and medium sized businesses (SMBs) need to have a Swiss Army knife of skills. The more tools they can add to it, the better their chance of building a strong foundation of growth. However, founders of tech companies are predominately technical themselves and can lack the business and financial acumen needed for success. Founders are often cash-strapped, limiting their ability to provide employees with the skills needed to strengthen or compliment their own.

Access to trusted business advisory services, provided by government or through a third party is vital to building the foundational business DNA for startups. Investing in a business advisory grants program will provide invaluable support to founders. By also supporting founders with business administration, it allows them to focus on developing their technology and servicing their customers.

'Whole-of-life' cyber security accelerator programs

Many generic accelerator programs accept cyber security technology founders into their programs, which ultimately adds significant benefits to the technology of other startup founders. With one of Australia's largest and most successful cyber security accelerator programs closing its doors in 2023 (CyRise), cyber security startups have reduced chances of finding investors and support to accelerate the commercialisation of their products and services.

Reshaping accelerator programs to the end-to-end lifecycle of a startup, including the funding environment, will enable Australian cyber security companies to become global market leaders. Founders can be provided with all the services, networks and support required in a single program, ultimately increasing the chances of success for the industry and the Australian economy.





Prioritise domestic procurement of cyber security products and services through a 'buy Australian first' approach

Expanding the domestic market

Many large companies and government agencies – both at the state and national level – are bound by strict procurement guidelines, designed to ensure reliable performance of contractors and protect the integrity of their networks. But the complexity and cost of these requirements pose a barrier for smaller and newly established companies, which are often defeated by larger rivals with more experience and resources. While strict compliance and procurement rules are necessary to protect high-risk business areas, more can be done to ensure a greater participation of startups and other small companies in providing cyber security products and services to government and big corporates.

Long term consistent support is required by all levels of government and multinational organisations to embrace Australian cyber security technologies as an enabler to their competitiveness. Through a collaborative and sustained approach to prioritising domestic procurement of cyber security products and services, the cyber security sector and all other vertical economic markets will benefit. Opportunities exist to include SMB targets for government procurement of cyber security products and services, as well as public or private sector incentives to pilot programs of sovereign technologies and encourage more partnerships between multi-national companies and Australian cyber security companies in the delivery of services.

2023–2030 Australian Cyber Security Strategy

The Strategy and corresponding 2023–2030 Australian Cyber Security Action Plan outlines the Australian Government's vision of becoming a world leader in cyber security by 2030. Through six cyber shields and over three horizons, the Australian Government has developed a path to achieving their vision. At a significant investment of AU\$586.9 million commitment to the Strategy, it falls silent on its investment into, or utilisation of, domestic cyber security services or solutions to meet its vision.

A co-design approach to many actions and inclusion of leading industry experts on committees and councils provides benefits for all voices to be heard as the Strategy actions are implemented. However, ensuring that cyber security services and products in support of the Strategy actions are predominately drawn from homegrown companies will have a significant impact to the domestic market. More importantly, it signals to the domestic market of strong validation in our own cyber security technologies – be it identity management, cloud hosting or threat intelligence.



Attract investment and improve innovation to support a rapidly maturing cyber security industry

Trusted seed funding

The crucial asset of a cyber security company is the Intellectual Property (IP) being built. It's the talented people of a startup that have the exciting job of building and creating some of the value of this IP. However, this can come at great expense to the company.

When there is little or no revenue being injected into a startup, or a company's revenue is on the cusp of a positive financial trajectory, it's important for the founders to raise those funds to be able to grow the technology and employ the required skills. There is a maze of information available on boot-strapping, angel investors, venture capitalists and debt-financing, accompanied by word-of-mouth referrals. Non-dilutive and non-debt sources of funding can be accessed through government grants, however, these are often accompanied with a matching co-contribution by the company which impacts cashflow.

Development of trusted investor funding programs by governments will build the cyber security industry and invest in the country's innovation, positioning Australia as a potential lead market player. Governments could also look at providing incentives to existing angel, private equity or VC funds when investing at pre-seed, seed or Series A raises for a cyber security company. Large industry players could support homegrown angels and VCs by way of investment into their fund, to secure the future of the maturing cyber security sector.

Short-term incentive boosts

It is estimated that the cyber security sector has generated \$3.99 billion of GVA in 2023 – an increase of 66 percent in 2022. As young as the cyber security sector is, it can no longer be classified as an emerging industry. With growth comes the next set of pain points, which requires flexibility in the implementation of short-term investments.

A key obstacle for many Australian cyber security companies, especially in services, is a lack of scalability in their business models. This means they cannot easily grow to capture opportunities and export relies on expanding their workforce offshore in ways that are often too difficult. Opportunities exist for consideration of a short-term boost to the cyber security sector which could include:

- increasing the Research and Development Tax Incentive for cyber security companies to capitalise on sovereign technology and boost positive cashflow in early-stage ventures;
- incentivising angel investors, private equity and venture capital funds to grow Australian funds and invest those funds directly into homegrown cyber security companies;
- encouraging public and private sector cyber security 'health check' or 'uplift' programs to utilise cyber security SMBs for the delivery of the service or products; and
- reshaping the 2023–2030 Australian Cyber Security Strategy's Cyber Security Industry Challenge initiative to include a commercialisation continuum to expand the customer base of a sovereign cyber security company.



Promote public-private partnerships to educate local cyber security talent, with a focus on attracting women, First Nations Australians and neurodivergent talent

Education and professional development pathways

With a significant demand for cyber security professionals, the growth in cyber security training programs, free and paid, has grown exponentially. However, a lack of clarity across the industry for the requisite skill sets, education and experience for a role is compounding the problem for those wishing to enter or transition into a cyber security career. These elements are producing a fragmented education and training pathway for cyber security.

Cyber security skills shortages in Australia could stem from certain shortcomings within our education and training systems. These systems may not currently offer comprehensive cyber security programs that adequately prepare professionals for the sector. Additionally, there's a lack of established frameworks to promote the availability of high-quality courses that align with a clear professional pathway. Furthermore, the existing training programs may require greater adaptability to swiftly respond to the ever-changing skill requirements within the cyber security sector. They should also be designed to cater to a diverse group of learners with varying backgrounds and needs.

Promoting awareness and clarity about the cyber security field and its career pathways is essential to attract learners from diverse backgrounds. Making the cyber security profession more appealing to women, First Nations Australians and neurodivergent talent is not only a matter of addressing diversity disparity, but also a strategic move to fulfill workforce demands effectively.

The development of a national framework (aligned with international standards) for the professionalisation of cyber security education and training would provide:

- candidates wishing to enter a cyber security career with clear guidance on what education and training they require from formal, non-formal or online education;
- employers with recruitment standards to advertise new positions or vacancies, managing expectations on both sides;
- requirements for vendors of cyber security training to align programs against the framework, providing transparency between cost and outcomes for the consumer; and
- cyber security companies who deliver hands-on real-world training environments with clarity in the development of holistic training programs.



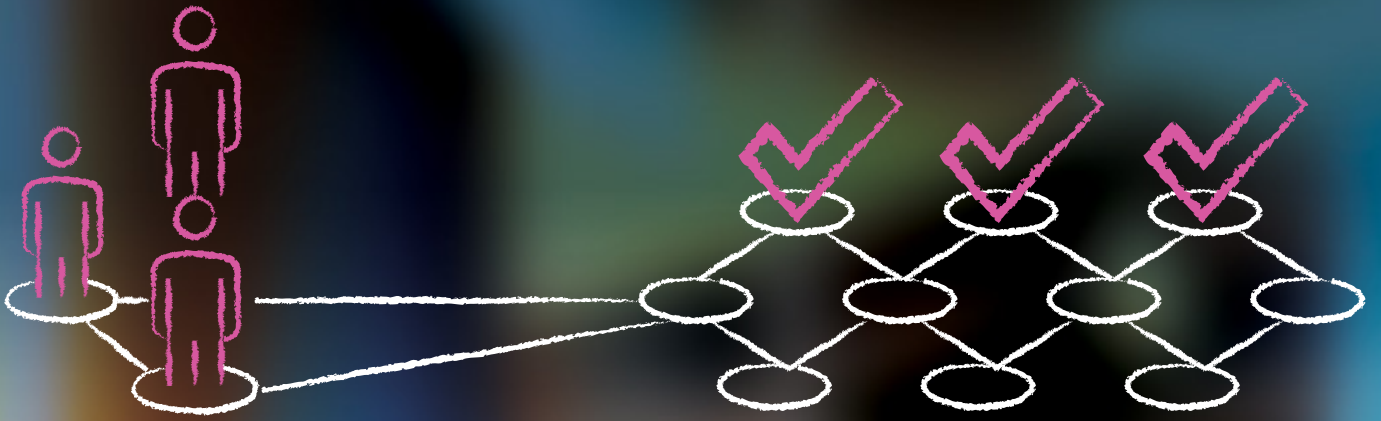
Significant demand for
cyber security



Australian cyber security
skills shortages



Changing skills requirements
within cyber security sector



Focused approach to workforce skills, diversity and funding

With limitations on the deployment of a clear, consistent and uniform education and training pathway, the cyber security gap continues to widen against demand. Except for the government's national TAFE fee-free courses, costs to learn or upskill into cyber security can disadvantage many potential candidates. Recruitment practices can also discriminate against those who do not have the 'recognised' accreditations or certifications due to the cost associated for enrolment and completion. Through the Cyber Security Skills Partnership Innovation Fund grants, the Australian Government's aim was to increase the diversity of the workforce through public and private partnerships; but there has been minimal publicly available information as to whether the aims have been achieved.

The 2023–2030 Australian Cyber Security Strategy outlines Shield 5 (sovereign capabilities) as an action item to grow and professionalise the cyber workforce through a three-tier approach of skilled migration, diversity and development of a framework. The Strategy outlines a strong foundation to address the cyber security workforce, however implementation will be the key factor to its success.

Under the auspices of the Strategy, a committee or a council will be established with a mandate to give effect to the workforce actions in the Strategy with a specific focus on:

- the development of a national professionalisation pathway from primary school to undergraduate degrees;
- advice to government, public and private sector on cyber security education, training and recruitment;
- facilitating public-private partnerships on cyber security education and training that focuses on delivering diversity outcomes rather than commercial outcomes;
- oversight on future government grants focused on cyber security skills; and
- supporting not-for-profit associations such as the Australian Women in Security and Australian Information Security Association who focus on attracting entry-level and transitioning members into the industry.



Special feature

The release of the 2023–2030 Australian Cyber Security Strategy

On 22 November 2023, the Australian Government released the 2023–2030 Australian Cyber Security Strategy (the Strategy). The Strategy is the federal government's AU\$586.9 million commitment to help realise the vision of becoming a world leader in cyber security by 2030.

The Strategy outlines six cyber shields:



1.

Strong businesses and citizens

\$290.8 million in support for small and medium business, building public awareness, fighting cybercrime, breaking the ransomware business model and strengthening the security of Australians' identities



2.

Safe technology

\$4.8 million in establishing consumer standards for smart devices and software



3.

World-class threat sharing and blocking

\$9.4 million to build a threat sharing platform for the health sector



4.

Protected critical infrastructure

\$143.6 million in strengthening our critical infrastructure protections and uplifting government cyber security



5.

Sovereign capabilities

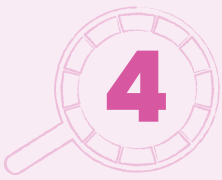
\$8.6 million in professionalising our cyber workforce and accelerating the cyber industry in Australia



6.

Resilient region and global leadership

\$129.7 million in regional cooperation, cyber capacity uplift programs and leadership in cyber governance forums on the international stage



The 2023–2030 Australian Cyber Security Action Plan supplements the Strategy and details the key initiatives and actions:

Shield 1

**Strong
Businesses
and citizens**



Co-design and collaborate with industry to:

- Legislate no-fault, no-liability ransomware reporting obligations
- Design best-practice principles to guide good cyber governance
- Legislate a limited use obligation for ASD and Cyber Coordinator to encourage open engagement in the early stages of a cyber incident
- Establish a new Cyber Incident Review Board for conducting lessons-learned reviews of significant cyber incidents

Small to medium business support including:

- Create cyber 'health-checks' program to offer advice and guidance
- Establish Cyber Security Resilience Services to build cyber resilience and provide support when an incident occurs

Education and training campaign including:

- Expand national cyber security awareness campaign
- Delivery of tailored cyber awareness campaign through a community grant program

Shield 2

Safe technology



Co-design and collaborate with industry to:

- Mandate cyber security standards for consumer grade smart devices
- Voluntary labelling scheme to measure cyber security standards of smart devices
- Voluntary cyber security code of practice in software development
- Voluntary data classification model for consistent communication of consumer data holdings

Embedding cyber security practices into:

- Safe and responsible use of AI
- Protection of datasets of national significance
- A national security risk framework for assessment of vendor products and services operating within Australia

Shield 3

**World-class
threat sharing
and blocking**



Create whole-of-economy threat sharing through:

- Establishing an Executive Cyber Council to improve threat intelligence sharing
- Enhance ASDs CTIS platform for threat sharing platform
- Launch a threat sharing acceleration fund to establish Information Sharing & Analysis Centres (ISACs) in low maturity sectors
- Encourage and incentivise industry to share threat intelligence

Scale threat blocking capabilities through:

- Establishing a National Cyber Intel Partnership between industry, academia and civil society on existing platforms
- Expand reach of threat blocking with telecommunication, ISPs and financial services

Shield 4

Protected critical infrastructure



Clarifying critical infrastructure regulation:

- Moving elements of Telecommunications Act to SOCI Act
- Clarifying obligations of data storage and processing sector providers under SOCI Act
- Protect critical data in 'business-critical' data storage systems

Cyber security obligations and compliance:

- Cyber security obligations for Systems of National Significance and compliance monitoring and evaluation framework for critical infrastructure
- Introduce 'all-hazards' consequence management power to allow government to direct an entity to take specific actions to manage nationally significant incident
- Expansion of National Cyber Security Exercise Program and develop incident response playbook
- Uplift cyber security in the commonwealth government to include zero trust culture, regular maturity reviews and map important digital infrastructure.
- Develop a whole-of-government approach to cyber skills in the APS and establish Defence Cyber College

Shield 5

Sovereign capabilities



Grow and professionalise cyber workforce through:

- Attracting skilled migrants to increase cyber skills pipeline
- Improving diversity of cyber workforce utilising recruitment practices
- Developing a framework for cyber security professionals

Accelerating cyber industry research and innovation through:

- Cyber Security Industry Challenge Program, leveraging DISR's existing initiatives

Shield 6

Resilient region and global leadership



Collective cyber resilience across Pacific and SE Asia:

- Refocus Cyber and Critical Technology Cooperation Program to support enduring cyber resilience and technology as well as strategy for diversity and inclusion
- Develop a framework for government and industry resources, including a regional cyber crisis response team
- Harness industry to pilot technologies across the region at scale

Shape, uphold and defend international cyber standards:

- Collaborate and advocate for international standards, rules of engagement and frameworks
 - Review attribution framework to publicly apply sanctions to those who carry out or facilitate malicious cyber incidents
-

Analysis







The cyber security sector generates and protects significant economic value for Australia. Reflecting the challenges and opportunities that define Australia's cyber security landscape, the Strategy will provide a positive step forward to bolstering our competitiveness in the global market. Acknowledgement needs to be given to the breadth of consultation undertaken by the federal government with industry experts, the call for public submissions and rolling national workshops in the development of the Strategy. It is a Strategy that may not meet the needs of everyone, however it has certainly provided ample opportunity for voices to be heard.

The growth barriers faced by the Australian cyber security sector in the global market are not new; and the sector faces enduring challenges that continue to be addressed in a piecemeal approach across public and private sectors. The Strategy aims to address some of these challenges:

- 1. Economic resilience:** A significant portion of the Strategy's funding has been committed to 'Strong businesses and citizens' (49.5 percent) whilst 'Safe technology' has been apportioned the lowest amount of funding (0.8 percent). A portion of Shield 1 funding is directed towards small to medium businesses, but it still represents a low investment in protecting and developing resilience of Australia's economic market.
- 2. Sovereign technologies:** Strengthening the cyber security maturity of government departments and agencies, a greater focus on national threat intelligence sharing and protecting critical infrastructure are outlined as key actions. This will provide positive impacts as a nationally coordinated approach for cyber defences. The Strategy falls silent on the development of sovereign secure-by-design cyber security technologies as well procurement of homegrown technologies.
- 3. Commercialisation:** The Strategy identifies the Cyber Security Challenge program as part of its investment into sovereign research and development. However, it is reliant on cyber security startups and small businesses to access existing federal government initiatives to grow their client base and contribute to the growth of the sector.
- 4. Skilled workforce:** Growing Australia's cyber security workforce is an ongoing and significant challenge we face, and one of the more complex issues to address. The Strategy supports existing federal government skills initiatives through the 2023 release of the Migration Strategy, a global outreach approach to attract highly skilled migrants to expand the skills pipeline.



Figure 20. Commitment of total Strategy funding against shields

	Shield 1 – Strong businesses and citizens	49.5%
	Shield 4 – Protected critical infrastructure	24.5%
	Shield 6 – Resilient region and global leadership	22.1%
	Shield 3 – World-class threat sharing and blocking	1.6%
	Shield 5 – Sovereign capabilities	1.5%
	Shield 2 – Safe technology	0.8%

Note: The funding represented in this table directly relates to the commitments in the Strategy and does not reflect broader whole of government spend on cyber security. The Shields that received less funding were because the consultation process determined that there was sufficient funding already on existing programs and the strategy focused on enhancing, continuing and building on those programs.

As highlighted in *Chapter 1: The global outlook for cyber security*, the Strategy is closely aligned with the objectives of the UK and US strategies. This is a positive step for Australia as it navigates global cyberspace with partner nations.

The Strategy is to be commended on its holistic approach to addressing the national and international cyber security threat environment and will provide much needed support to the growth trajectory of the Australian cyber security sector. We look forward to the implementation of the Action Plan over the next seven years.

Chapter 5: The role of AustCyber



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

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

AustCyber has been leading significant efforts to accelerate and sustain Australia’s cyber security sector, including vital activities to counter the challenges highlighted earlier in this plan.

AustCyber has three focus areas:



**1. Grow and connect
Australia’s cyber
security ecosystem**



**2. Promote and export
Australia’s cyber
security to the world**



**3. Help make Australia
the leading centre for
cyber security education**

In 2023, several programs and initiatives were run to deliver on these focus areas.

Through these initiatives, AustCyber continues to strengthen the national cyber security sector – championing innovation, growth and global competitiveness.

Australian Cyber Security Professionalisation Program

AustCyber led an industry co-design team to create the Australian Cyber Security Professionalisation Program (ACSP) in collaboration with key stakeholders – including universities, TAFEs, cyber security experts, industry associations and professional bodies.

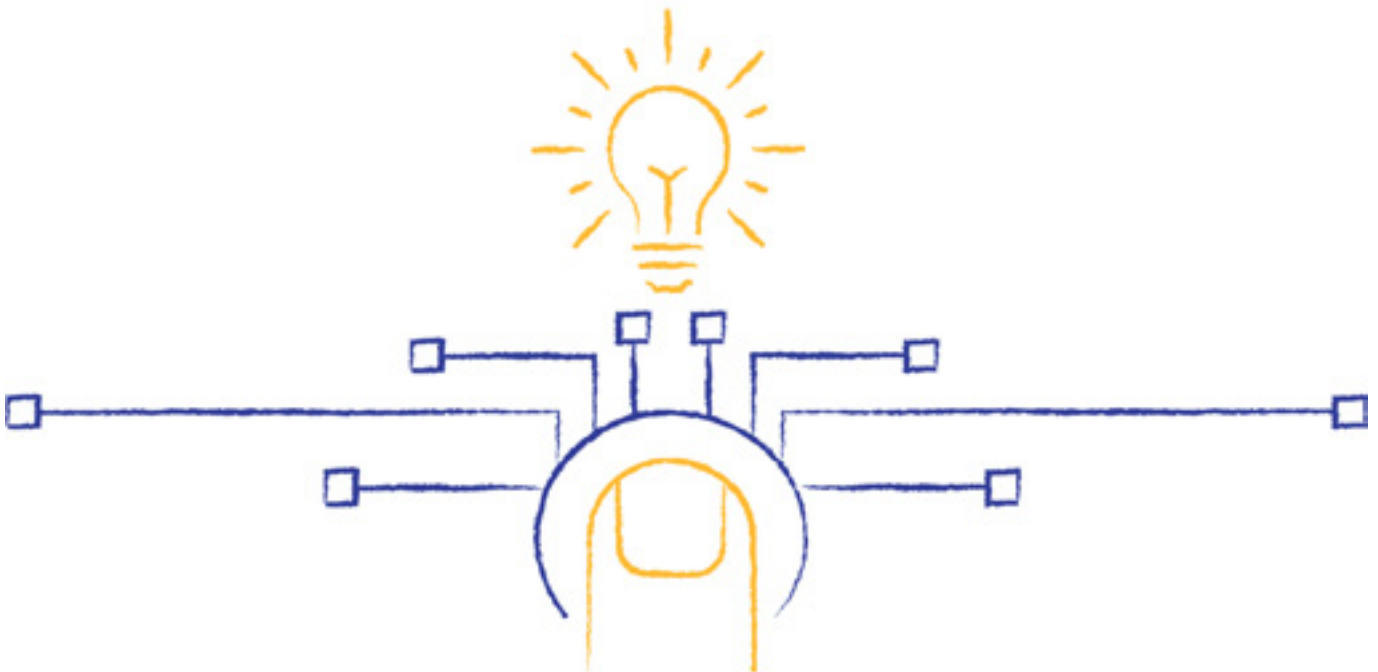
The ACSP program is focused on the development and implementation of globally aligned professional standards and a professional recognition scheme that will provide the existing and future cyber security workforce with choice and clear career pathways to guide them on their career journey. It will provide clarity and guidance for employers when identifying their cyber security needs. It will also protect the community by ensuring that recognised cyber security professionals are well-trained, experienced and competent; and adhere to a code of ethics that prioritises safeguarding the public's information and digital assets.

ACSP is a critical step in professionalising the cyber security sector in Australia to global standards, with the intent of being a world leader and improving trust and confidence in Australian cyber security professionals.

AustCyber Innovation Network

The AustCyber Innovation Network, which will spread across metropolitan and regional areas in Australia, is poised to stimulate innovation, fortify cyber security communities and offer a unique collaborative platform to stakeholders across the sector.

By expanding the footprint of the Innovation Network across the country, it will help increase accessibility of cyber security support for under-served and under-represented regions and groups. Through the AustCyber Innovation Network, AustCyber is committed to providing unwavering support to the cyber security needs of all, including startups, scaleups, small to medium businesses, large enterprise and government.



AustCyber Projects Fund

The AustCyber Projects Fund was a AU\$15 million, three-year initiative aimed at fostering the growth of Australia's cyber security industry and promoting global innovation.

To simplify the application process, two project categories were introduced. Proposed projects could either address specific 'sector challenges' vital for the growth of Australia's cyber security sector or focus on broader objectives.

All proposed projects secured matched industry funding. The fund supported projects aligned with merit criteria, including those addressing specific problem statements aimed at enhancing Australia's cyber security infrastructure.

The complete list of beneficiaries from the projects fund is below:

Projects

AARNet – SOC services

Airlock Digital – Application whitelisting

Alpha Beta College – AUCyberExplorer

Cybermerc – AUSHIELD

Cybermerc – RedZenit

Cynch Security – Cyber Fitness platform

FifthDomain – Cyber Security Skills and Technology Accelerator Project

Forticode – Cipherise™

Grok Academy (formerly ACA Challenges) – Schools Cyber Security Challenges

HackHunter – Pursuit Portable WiFi Tracker

Haventec – Project Todd

Laava ID – Smart Fingerprint®

Locii – truuth Identity Platform

Penten – The Playbook

Penten – Secure Network as a Service (SNaaS)

Penten, WorldStack and **CyberCX** – HoneyTrace

QuadIQ – Intelligence Trust Evaluation System (ITES)

South Metropolitan TAFE – TAFEcyber

The University of Adelaide, CSER Group – Cyber Security Teacher Professional Learning

Untapped – Cyber Security Training and Assessment Centre

Vault Cloud, QuintessenceLabs and **Ziroh Labs** – Project Acredo

WithYouWithMe – WYWM Cyber Security Analyst Course



AUCYBERSCAPE

AUCyberscape is Australia's first national cyber security digital ecosystem. It's a 'one-stop-shop' for businesses, government, investors and individuals to better understand cyber security, explore the Australian sector and connect with the cyber security companies or products and services they may be looking for.

AUCyberscape provides a platform for Australian cyber security companies to showcase their products and services, connect with customers and access information to support their company development and growth. There are over 315 Australian cyber security companies featured on the platform.

This digital ecosystem is a valuable resource for anyone who is interested in cyber security, whether you are a business owner, a government official, an investor, or an individual.

Since its inception, AUCyberscape has been a pivotal source of data and information in the drafting of AustCyber's Cyber Security Sector Competitiveness Plans. The data fields contained within AUCyberscape is information that is not collated elsewhere and provides a more detailed and deep-dive analysis of the cyber security industry and its growth.



AUCyberExplorer is an interactive tool that tracks the state of the Australian cyber security job market by providing detailed, actionable data about cyber security job supply and demand and career pathways.

The website has the following features:

-
- **Supply and demand maps** – interactive geographical maps and charts that visualise data on the supply and demand for the cyber security workforce across Australia. This includes current, forecast, historical and international comparison. You can use this tool to identify the size of the workforce, including age, gender and organisations' demand for different roles.
 - **Career pathways** – an interactive visualisation that shows the relationships between roles, certifications and skills.
 - **Top roles** – lists the top cyber security roles in Australia, along with the skills and certifications required for each role.
 - **Certifications** – lists the most in-demand cyber security certifications in Australia.
 - **Glossary** – provides a glossary of terms related to cyber security.
-

AUCyberExplorer is a valuable resource for anyone who is interested in the Australian cyber security workforce, including job seekers, employers, education providers and policymakers.



Appendix A: State of the states



Overview

In 2020, the ACT Government set a goal to recover all jobs lost during COVID, then to grow the labour market to achieve 250,000 jobs in the territory economy by 2025. The ACT has now hit that goal with over 265,000 people working across the territory. The ACT Government has since reset the jobs target to grow the total labour market to an ambitious 300,000 jobs by 2030.

In contributing to achieving this target, the ACT Government is focused on further elevating Canberra as a leader in cyber security in Australia. Canberra is home to the highest density of prime contractors, cyber SMEs, cyber prime contractors and Australian Government agencies. Canberra has highly ranked universities and institutions offering cyber security education from certificates to PhDs, through the Australian National University (ANU), University of Canberra (UC), University of New South Wales, Canberra (UNSW Canberra), Canberra Institute of Technology (CIT) and private sector providers. Canberra also has the highest levels of security clearances among the most educated cyber workforce in the country.

Initiatives

Proving its commitment to growing cyber security in the ACT, the ACT Government founded the Canberra Cyber Hub in 2021 to establish and position Canberra as a leading hub for cyber security in Australia. By fostering collaboration among industry, research institutions and stakeholders, the Canberra Cyber Hub drives business growth through developing a skilled workforce, encouraging innovation, and maximising opportunities for meaningful engagement between cyber businesses and potential customers. Canberra Cyber Hub achieved notable successes in the 2022–23 FY, including:

- The *Closing the cyber skills gap – work-integrated learning pilot* was co-designed with Canberra cyber employers, tertiary education and training providers, in collaboration with the Digital Skills Organisation, to help address the cyber skills gap and deliver work ready employees to employers.
- The *Cyber career symposium* event featured a cyber career showcase with 21 Canberra businesses and education and training providers.
- The *Sovereign Cyber Capability Unlocked* breakfast event showcased 15 Canberra cyber companies to prime contractors and global supply chain primes.
- The *Cyber skills activation campaign* enabled over 800 mid-career professionals to engage with the Canberra Cyber Hub to learn more about how they can transition to a career in cyber security.

New South Wales

Overview

The 2021 NSW Cyber Security Strategy is a three-year plan that outlines the NSW Government's vision for NSW to become a world leader in cyber security: protecting, growing and advancing our digital economy.

The four commitments that make up this strategy include:

- Increase NSW Government cyber resiliency
- Help NSW cyber businesses to grow
- Enhance cyber security skills and workforce
- Support cyber security research and innovation

The NSW Cyber Security Strategy is a comprehensive plan that aims to make NSW a safe place in Australia to live, work and do business online. The Strategy is targeted at meeting the needs of government, business and citizens for connected, protected and trusted services and infrastructure.

The NSW Cyber Security Policy sets out the mandatory requirements for NSW Government departments and agencies to manage cyber security risks to their information and systems.

Initiatives

To further grow capability in the cyber security sector, the NSW Government has created a Cyber Hub to continue to drive the sector's growth. Its programs include:

- The *Cyber Ambassador program* and *Cyber Industry Experience program* for high school students across NSW to drive awareness of and interest in, cyber security career paths.
- The *Cyber Health Clinic program* which helps to prepare small to medium enterprises to face growing cyber threats and address skills gaps by providing future cyber professionals with job-ready experience. Selected university students will conduct the checks under supervision and gain invaluable industry experience.
- The *NSW Cyber Business Exchange program* which brings together businesses across multiple sectors, to foster collaboration and communication between different sectors, to ensure all parties are sharing knowledge and increasing their cyber capabilities, as well as market opportunities for NSW cyber businesses.

Overview

Since 2019, the NT Government has delivered a substantial cyber security awareness program for small businesses, government staff and the local ICT industry. The program has been open to the public, with briefings provided in city and regional centres. This has enabled a range of digital programs to be incrementally created that are tailored to specific audience groups, needs and skill levels.

Moving cyber security education into a digital program will continue to enable the NT Government to reach a wider audience and will allow business owners, community groups and interested people to work through the information when and where it is convenient for them.

Initiatives

- In 2021, the government opened the *Joint Cyber Security Services Hub (JCSS)*. The Darwin-based JCSS serves as a collaborative hub between the territory, federal government and the local ICT industry, addressing the 'real and present danger of threats to cyber security through targeted and expert training'.
- Without having endorsed a formal cyber security strategy, the government is actively initiating deliverables which will expand the current scope of how the territory develops and interacts with cyber security skills and how skilled migration visas impact the current pipeline of the cyber security workforce.

Queensland

Overview

The Queensland Government's Cyber Security Unit sets their cyber security policy and guidance for the public sector, including managing a number of government cyber security services and developing a public sector cyber workforce.

Currently, the government is developing a formal Digital Economy Cyber Security Strategy, whilst progressing a number of government and private sector initiatives and priorities to improve the current state of the sector within Queensland.

Initiatives

- The Queensland Government is collaborating with TAFE QLD to produce and improve the critical skills shortage through a *cyber skills accelerator program*.
- Sunshine Coast – the new *international broadband (submarine) cable* that is fast tracking digital capability on the Sunshine Coast.
- CI-ISAC: *Critical Infrastructure Information Sharing and Analysis Centre* (Sunshine Coast) – a collective cyber defence for critical infrastructure.
- *AusCert* is successfully being run out of the University of Queensland – delivering Queensland's largest cyber conference.



South Australia

Overview

The South Australian Government has four key areas of focus for its cyber security sector. The first focus area is promoting the capabilities of South Australia's cyber security industry. This involves showcasing the capabilities of local companies through ongoing updates to the cyber capability matrix document annually. It also includes conducting insight programs to showcase company capabilities to a wider audience through the digital hub.

The second focus area is growing and innovating the cyber security sector in South Australia. Initiatives to support this include helping startups and scaleups commercialise new solutions through various programs. It also involves partnering cyber security companies with research teams and universities. The third focus area is preparing for the delivery of major initiatives like the AUKUS agreement. To support this, the government is focused on ensuring South Australia has a robust cyber security industry that can deliver on agreements such as AUKUS.

The final focus area is developing skills and talent for the cyber security sector. Initiatives include offering defined pathways into cyber careers with a variety of training offerings such as cyber security certification courses through TAFE SA (for example, the Cert IV in cyber security). It also includes talent programs such as The Alternative which offers SMEs within growing industries such as tech, cyber, energy and space, access to a pool of graduates on six month rotations.

Initiatives

- Building local skills and the talent pipeline through increased and diverse pathways and training. This includes certification courses such as the *Certificate IV in Cyber and Diploma of Cyber* at TAFE SA, and supporting innovative skilling organisations such as *42 Adelaide* (a free coding school).
- Preparing for agreements like AUKUS and ensuring a robust local industry which aims to position South Australia as a trusted partner of choice.
- The recently launched *Cyber Uplift Step Program (CUSP)* with the Australian Cyber Collaboration Centre, based in Adelaide's Lot Fourteen innovation precinct. This is aimed at addressing integration of cyber across different sectors by providing an affordable and accessible program for small businesses.

Overview

The Tasmanian cyber security sector is relatively small, but is rapidly maturing to grow resilience and capability to protect Tasmanian data and information, and ensure security in the delivery of essential services. As outlined in the Tasmanian Technology Sector Scan, the Tasmanian State Service (TSS) is a leading employer of digital skills in Tasmania, which includes cyber and information security skills. Supported by the Australian Government's whole of country SFIA license, the TSS through the Department of Premier and Cabinet has commenced development of a digital workforce capability framework and roadmap for workforce planning, recruitment and deployment of staff, career pathway planning and skills assessments.

The Tasmanian Government Cyber Team is implementing the Tasmanian Government's AU\$4.9 million four-year Cyber Security Uplift Program to improve their ability to protect citizen data and minimise the disruption of critical services. The Cyber Team is also responsible for the Tasmanian Cyber Security Policy (2022) and the soon to be released Tasmanian Government Cyber Strategy 2023–2027. The new policy focuses on enabling a digital future through trust and resilience through leadership, security of government services and partnerships.

Initiatives

- The University of Tasmania offers *cyber security specialisation* options aimed at graduating cyber workforce professionals and leaders in the Associate Degree in Applied Technologies, Diploma and Undergraduate Certificate of ICT Professional Practice, Bachelor of Information and Communication Technology (BICT) and Master of Information Technology and Systems (MITS).
- The TasTAFE *Cyber Innovation Training Hub* received AU\$1.45 million in 2021 from the Cyber Security Skills Partnership Innovation Fund to establish a cyber training facility. The Cyber Hub offers cyber skills development and career pathways for new entrants and career changers. The Certificate IV in Cyber Security commenced in July 2023 as part of this initiative.
- Tasmania has a rich *community of practice* that supports the cyber workforce and government initiatives. This includes the TasICT Cyber conference, Australian Women Security Network (AWSN) Tas chapter events and training, Australian Information Security Association (AISA) branch meetings, Splunk and SecTalk meetups, Australian Computer Society events and membership to name a few.

Overview

Victoria's Cyber Strategy 2021 sets the Victorian Government's five-year vision for a cyber safe Victoria, positioning Victoria as a global industry leader in cyber security by fostering a skilled workforce and innovative local sector that enhances cyber resilience across government, industry and the community.

The vision is underpinned by three core missions: the safe and reliable delivery of government services (mission 1); a cyber safe place to work, live and learn (mission 2); and a vibrant cyber economy (mission 3). These missions are supported by annual Delivery Plans, which set out priority actions to advance the Strategy's vision.

The Strategy was released in 2021 with an initial investment of AU\$50.8 million in funding, with an additional AU\$34.7 million investment announced in the 2023–24 Victorian Budget to establish a cyber defence centre and emergency management capability.

Initiatives

- Establishing the *Cremorne Digital Hub* as the gateway to Victoria's digital ecosystem and growing the cyber sector.
- Backing Victoria's *startup and scaleup ecosystem* through Launch Victoria and Breakthrough Victoria.
- Supporting Victorian cyber businesses to thrive locally and internationally and *attracting global investment* in cyber to Victoria through Global Victoria and Invest Victoria, Victoria's trade and investment agencies.
- Putting Victoria on the international stage by *sponsoring the Australian Cyber Conference*, the largest cyber conference in the southern hemisphere.
- Providing opportunities for Victorians to become qualified in cyber through the *Free TAFE* initiative.
- *Free online courses and workshops* to help Victorian businesses gain a deeper understanding of cyber security risks and mitigation strategies, complemented by free interactive webinars on cyber security.
- Upskilling mid-career Victorians and supporting them to move into digital and cyber careers through the *Digital Jobs Program*.
- Developing job-ready cyber skills by matching digital tertiary ICT students and graduates with Victorian businesses to solve tech and cyber challenges through *SummerTech LIVE*.
- Widening the pipeline of talent by increasing the diversity of the cyber workforce through the *Women in Security Program*, co-developed by the Victorian Government and the Australian Women in Security Network (AWSN).

Western Australia

Overview

The WA Government is continuing to increase its efforts to build and support the ability to protect its data, assets and service delivery from cyber threats. The Office of Digital Government (DGov) is leading the sector to detect and effectively respond to cyber threats while supporting state government agencies to improve their own cyber capabilities. DGov works closely with academia and the local cyber security industry, including CyberWest to support innovation and build skills in WA.

Initiatives

- *Uplifting the cyber security capabilities of the public sector* and supporting the implementation of the controls through the WA Government Cyber Security Policy.
- *Building and retaining skills* by working collaboratively with the academic sector, students are provided with internship opportunities within government. DGov has facilitated more than 150 students through various work integrated learning programs over recent years. DGov also provides training opportunities to the WA government agencies to ensure the sector remains skilled in awareness and capabilities in addressing ongoing cyber security threats.
- *Improving visibility of threats and vulnerabilities* across the public sector through the WA Government Security Operations Centre (WASOC) with 88 WA government entities connected. WASOC also engages with industry and federal intelligence partners to ensure the WA public sector remains aware of current cyber security threats.
- *Implementing the Digital Strategy* for the Western Australian Government which sets out four strategic priorities for digital transformation in the state including 'Safe and Secure' which aims to protect services and systems from cyber threats and misuse.
- Participating in and administering the *Cyber Security Cooperative Research Centre (CSCRC)* for over seven years to December 2024. The CSCRC is responsible for 93% of national cyber security funding. DGov has led 29 projects, administering the national collaboration which includes seven research institutions, six governments or agencies and 11 industry organisations (including critical infrastructure). These projects range from promoting education and awareness to developing AI products to enhance cyber security capabilities.
- *Supporting the startup community and vendors* through regular industry engagement sessions to give local cyber security organisations a face-to-face briefing on the DGov cyber security projects and priorities and for DGov to find out more about the various services and specialities offered by these organisations.

Appendix B: Cyber security taxonomy



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

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 and intrusions, whether targeted or opportunistic.



Systems security: Operational, network and systems security that includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.



Software and platform security: Security that focuses on keeping software and an entire computing platform and devices – including mobile, cloud and web applications – resilient to cyber threats. This includes information security that protects the integrity and privacy of data, both in transit and at rest.








Attacks and defences: A proactive and adversarial ‘attack’ approach to protecting against cyber attacks, which includes penetration and vulnerability testing as well as ethical hacking. Defensive security focuses on reactive measures such as patching software and detection.



Human, organisational and regulatory aspects: Tools and services to protect against intentional and unintentional user mistakes; support observance of organisational governance and policies; and enforce compliance with regulatory requirements.

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

Cyber security product categories

Segment of the cyber sector	Examples
 <p>Infrastructure security</p>	<ul style="list-style-type: none"> • Managed security service provider • Security operations centres • Security hardware and physical systems
 <p>System security</p>	<ul style="list-style-type: none"> • Cryptography • Operating systems, network, cloud, quantum control and autonomous systems security • Authentication including biometrics • Identity access management
 <p>Software and platform security</p>	<ul style="list-style-type: none"> • IoT security • Software as a service (SaaS) • Threat intelligence analytics • Mobile, web and application security
 <p>Attacks and defences</p>	<ul style="list-style-type: none"> • Penetration testing • Bug bounty programs • Threat detection and response • Wargaming and exercising • Cyber deception technologies • Digital forensics
 <p>Human, organisational and regulatory aspects</p>	<ul style="list-style-type: none"> • Governance, risk and compliance management • Readiness and maturity audits • Privacy impact assessment • Training and education • Cyber-related professional services

Appendix C: Methodology



2023 Australian Cyber Security Sector Survey

AustCyber conducted the 2023 Australian Cyber Security Sector Survey of leaders and founders working in the sector.

Responses were collected via targeted messaging and convenience sampling through AustCyber’s network. 109 responses were collected between 9 August and 14 September 2023. Importantly, this is not a representative sample of the whole Australian cyber security sector, but do contain views from experienced voices within the Australian cyber security sector.

Of the 109 responses:

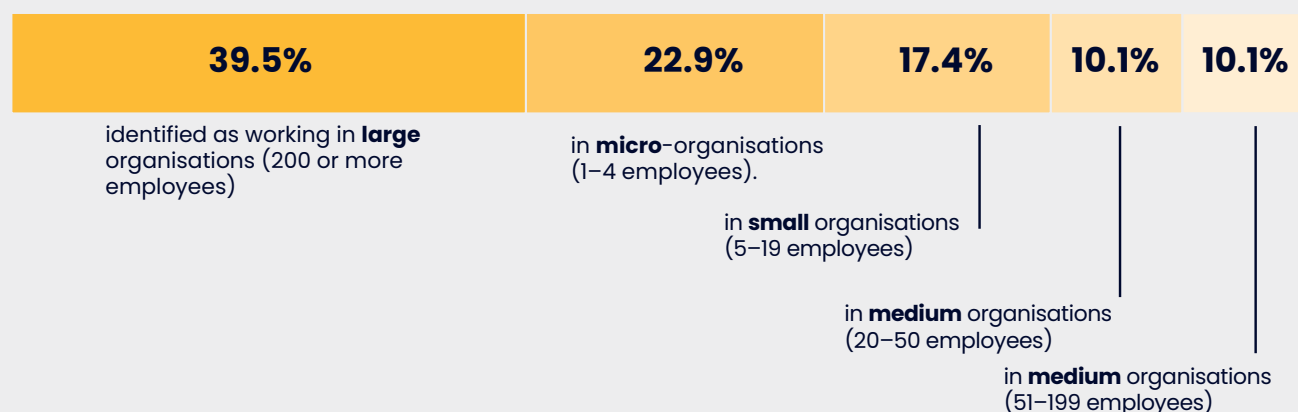
58 identified themselves as either a CISO or CEO/founder of a cyber security firm.

50.5% of respondents identified as having been involved in the cyber security sector for more than 10 years.



39.5% identified as working in large organisations (200 or more employees).

22.9% in micro-organisations (1–4 employees).



Survey data has been represented in three formats:

- Percentages of responses (%)
- Average value of ranked responses (n/n)
- Responses provided as free text

The average value i.e. n/6 requested responses that required a ranking of importance or impact. 'n' represents the value of responses and /6 represents the number of options offered.



AUCYBERSCAPE

AUCyberscape is Australia's first national cyber security digital ecosystem. It is a valuable resource for anyone who is interested in cyber security, whether you are a business owner, government official, investor or individual.

Since its inception, AUCyberscape has been a pivotal source of data used in the drafting of AustCyber's annual Cyber Security Sector Competitiveness Plan. The data fields contained within AUCyberscape provide information that is not collated elsewhere, enabling a more detailed and deep-dive analysis of the cyber security industry and its growth.

AUCyberscape collects data that includes:

- General business registration
- Company size and workforce
- Product and service categories
- Training category services
- Customer industries and export industries



Oxford Economics Australia

The 2023 Cyber Security Sector Competitiveness Plan drew upon the expertise and analysis of Oxford Economics Australia. This analysis came from multiple data sources:

Australian Bureau of Statistics' (ABS) Labour Force Survey (LFS)

"6291.0.55.001 – EQ08 – Employed persons by Occupation unit group of main job (ANZSCO), Sex, State and Territory, August 1986 onwards", ABS, accessed on 08/09/23, <https://www.abs.gov.au/statistics/labour/employment-and-unemployment/labour-force-australia-detailed/latest-release>. Data used from Jan. 2015 onwards.

2021 Australian Census

"6-digit level OCCP Occupation", ABS 2021 Census, accessed 07/09/2023, data accessed using ABS's Table Builder tool.

ABS' Industry Report

"81550DO002_202122 Australian Industry, 2021–22", ABS, accessed on 05/09/2023, <https://www.abs.gov.au/statistics/industry/industry-overview/australian-industry/latest-release#data-downloads>.

ABS' Input-Output Tables

"5209.0.55.001 Australian National Accounts: Input-Output Tables 2020–21", ABS, accessed on 11/09/2023, <https://www.abs.gov.au/statistics/economy/national-accounts/australian-national-accounts-input-output-tables/2020-21>.

JSA employment data (NERO)

"Nowcast of Employment by Region and Occupation, ANZSCO 4 Digit Occupations and SA4 Regions", Jobs and Skills Australia, accessed 05/09/2023, <https://www.jobsandskills.gov.au/data/nero#releases>.

Education enrolments and completions data from the Department of Education

Enrolments and completions data sourced directly from the DoE. <https://www.education.gov.au>. Data used from 2001 onwards.

NCVER

Custom data request processed through NCVER databuilder tool. <https://www.ncver.edu.au/research-and-statistics/data/databuilder>. Data used from 2001 onwards.

2022 AUCyberExplorer data collected by Stone & Chalk Group

Data provided directly by Stone and Chalk to Oxford Economics Australia in September 2023. Data used for wages calculation collected in March 2023.

Oxford Economics Australia has estimated two key areas:

- Labour – the Australian cyber security labour force over time, as well as the skills shortage that needs to be overcome to reach full employment in the sector.
- GVA – the GVA contribution of the Australian cyber security sector over time.

Gross Revenue of the Australian cyber security sector

- Used labour estimate to derive total workers, as the first stage of wage bill calculation.
- Calculated total gross wage bill for private and public sector workers. Wages derived from AUCyberExplorer Data, collected in March 2023.
- Divided the public and private gross wage bills by wage to revenue ratios based on ABS data to derive total gross revenue.
- Gross revenue to wage ratios derived from the ABS 2018–19 Input Output (IO) tables (public sector) and ABS' Australian Industry (2021–22) publication (private sector).

Gross Value Add of the Australian cyber security sector

- Gross revenue estimate from above calculation used as the first stage of GVA calculation.
- Sum of public and private sector GVA, then calculated by applying the GVA to gross revenue ratio to the gross revenue estimate.
- GVA to gross revenue ratios derived from the ABS 2018–19 IO tables (public sector) and ABS' Australian Industry (2021–22) publication (private sector).

Forecasted Gross Value Add of the Australian cyber security sector

- This was done based on monthly estimates and then forecasted using a random walk model equivalent to a seasonal ARIMA with a drift/trend component.
- Given the abrupt trends observed in some states in terms of employment and GVA, such as in South Australia, forecasting was limited to series at the national level which exhibit a clear, recognisable seasonal pattern.

The Australian cyber security labour force

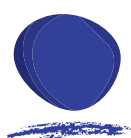
Defining the Australian cyber security labour force as members of the labour force who are classified by ANZSCO as being ICT Security Specialists, or Database and Systems Administrators and ICT Security Specialists. These are people classified under the following ANZSCO 6-digit codes:

- 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.

As part of providing a greater level of detail on cyber security labour force data, the following definitions have been utilised:

Dedicated	Roles with a dedicated focus on cyber security
Related	Roles requiring skills related to cyber security
Core	Derived from Dedicated Roles however are purely technical cyber security expertise only

- Labour force derived from the LFS Survey by ANZSCO Code. Focused on code 2621 – Database and Systems Administrators and ICT Security Specialists.
- Used the ratio derived from the 2021 Census of ICT Security Specialists (~40%) to the total 2621 labour force to estimate the number ICT Security Specialists.
- ANZSCO classifications were updated in November 2022.



AustCyber
Part of the Stone & Chalk Group

Contact

Email: **info@austcyber.com**

Website: **www.austcyber.com**

LinkedIn: **[AustCyber](#)**