# Upskilling and Expanding the Australian Cyber Security Workforce

A report by Per Capita for CyberCX

September 2022

CyberCX

percapita

FIGHTING INEQUALITY IN AUSTRALIA

# Table of Contents


About Per Capita ..... 3
About the Author ..... 3
About CyberCX ..... 4
Scope of Research ..... 5
Research Approach ..... 6
**Introduction ..... 7**
**An Overview: the Cyber Security Workforce ..... 9**
Existing Cyber Security and ICT Sector Workforce Dynamics ..... 9
REDSPICE and National Security Workforce Dynamics ..... 12
Cyber Security Sector Specific Skill Requirements ..... 12
**Cyber Training Pathways ..... 14**
Analysis of Educational Pathways into Cyber Security Careers ..... 14
University Pathways ..... 14
TAFE Pathways ..... 15
Graduate and Student Sentiment and Completion ..... 15
**The Cyber Skills Crunch ..... 16**
Modelling the Workforce Shortfalls in Cyber Security and ICT ..... 18
Trends in Completion Rates: TAFE ..... 19
Trends in Completion Rates: Universities ..... 20
Trends in Paid Employment and Sector Size Estimates ..... 21
Estimating the Graduate Cohorts and Sector Attrition Effects ..... 23
Graduate Outcomes, and Upskilling/Reskilling opportunities ..... 25
**Solving the Cyber Skills Shortage ..... 27**
Overview: The Role of TAFE ..... 27
Overview: The Role of the Universities ..... 27
Overview: The Role of the Private Sector-Sponsored Academies ..... 28
Migration in the Mix ..... 30
**Recommendations ..... 32**
**Conclusion ..... 33**
**Appendix 1: Analysis of sector specific recruitment challenges and prospective 'crowding out' effects ..... 34**
**References ..... 35**

## About Per Capita

Per Capita is an independent progressive think tank, dedicated to fighting inequality in Australia. We work to build a new vision for Australia based on fairness, shared prosperity, community, and social justice.

Our research is rigorous, evidence-based, and long-term in its outlook. We consider the national challenges of the next decade rather than the next election cycle. We ask original questions and offer fresh solutions, drawing on new thinking in social science, economics, and public policy.

Per Capita's operating model is to invest in highly qualified researchers who work on applied policy development, rather than the more abstract, theoretical approaches of academia. Our audience is the interested public, not just experts and policy makers. We engage all Australians who want to see rigorous thinking and evidence-based analysis applied to the issues facing our country's future.

## About the Author

### Dr. Michael D'Rosario, Research Economist

Michael is an economist/econometrician and strategy advisor, with experience working with NFP, university and corporate organisations in Australia and abroad. Most recently, Michael served as chair of Financial Markets at Deakin University, the manager of a large research program affiliated with the University of Melbourne, the ESG/Impact Advisor to CPA Australia, and as Research, Policy and Communications Advisor to the Victorian Aboriginal Legal Service and the National Aboriginal and Torres Strait Islander Legal service. Prior to these roles, Michael worked with PwC, KordaMentha, AusAid, Victoria University and the University of Melbourne. Michael has served on a number of university boards as a Non-Executive Director and Deputy Chair.

Michael's expertise is in non-parametric estimation, ensemble forecasting, understanding and evaluating complex economic relationships and in explainable/ethical uses of machine learning. Michael's early work focused on Australia's ICT/computing legacy; and on factors that determining infringing behaviours in digital markets and commerce, as well as the prediction of infringing behaviours. Michael's doctoral and postdoctoral work in econometrics has focused on the role of innovation in driving job creation, economic development, and services access.

## About CyberCX

CyberCX is the leading provider of professional cyber security services across Australia and New Zealand.

With a workforce of over 1,200 professionals, we are a trusted partner to private and public sector organisations helping our customers confidently manage cyber risk, respond to incidents, and build resilience in an increasingly complex and challenging threat environment.

Through our end-to-end range of cyber capabilities, CyberCX empowers our customers to securely accelerate opportunities in the digital economy.

CyberCX's end-to-end services include:

- Consulting and advisory
- Governance, risk, and compliance
- Incident response
- Penetration testing and assurance
- Network and infrastructure solutions
- Cloud security and solutions
- Identity and access management
- Managed security services

## Scope of Research

This report tracks and analyses the emerging cyber security needs of Australian firms, paying particular attention to the skills and capabilities of the workers already employed in this crucial sector, and the increasing demand for their work. Our analysis considers the anticipated shortfalls that are looming within the sector and considers current and expected graduation rates and questions concerning international migration and its relationship to the skills and training system. Additionally, we explore alternative training models that could address sector specific needs, particularly those that provide public/private partnering and emphasising practical learning.

In particular, the report identifies the gaps clearly visible within Australia's cyber security training and education frameworks and outlines new alternative articulation pathways that could address existing skills shortages, as well as exploring several emergent models of training that emphasise practical skills acquisition. Crucially, this report emphasises the critical role that an investment in adequate skills and training plays in addressing Australia's increasing cyber security needs.

A further set of analyses to be published within a forthcoming research report consider the broader costs and impacts of cyber crime and highlight key evidence that shows the full cost of failing to address this critical workforce shortage. The forthcoming report explores key trends in cyber crime, analysing social, economic and diplomatic/sovereign impacts. The analyses consider the national policy responses to cyber crime and the principal legislative responses to cyber crime, as well as the emerging role of key agencies responding to the emerging challenges of cyber crime.

## Research Approach

In formulating a viable and appropriate research strategy, we engaged in a series of consultations with several longstanding cyber security industry recruiters and stakeholders across cyber security sector, academia and relevant divisional units of CyberCX.

### Presentation of Research Strategy and Methodology to Stakeholders

Upon establishing a viable research framework, we initiated a consultation process with representatives of the cyber security community. During these consultations we outlined the following:

- The methodological approaches proposed for the research;
- The availability of different data sources (and those that required specific permissions); and
- The approaches available for the dissemination of research.

We obtained feedback from the group and sought to reflect this feedback in the research methods to the extent appropriate.

### Research Reference and Advisory Group

While conducting this research, we sought feedback from, and consulted with, experts from our internal reference group. The reference group informed the following aspects of the research:

- Offering insights into the viability of the research approaches;
- Providing support in securing key third party datasets; and
- Supporting the communication and dissemination of findings.

### Members of the Research Reference and Advisory Group

We would also like to acknowledge the significant efforts of the reference group.

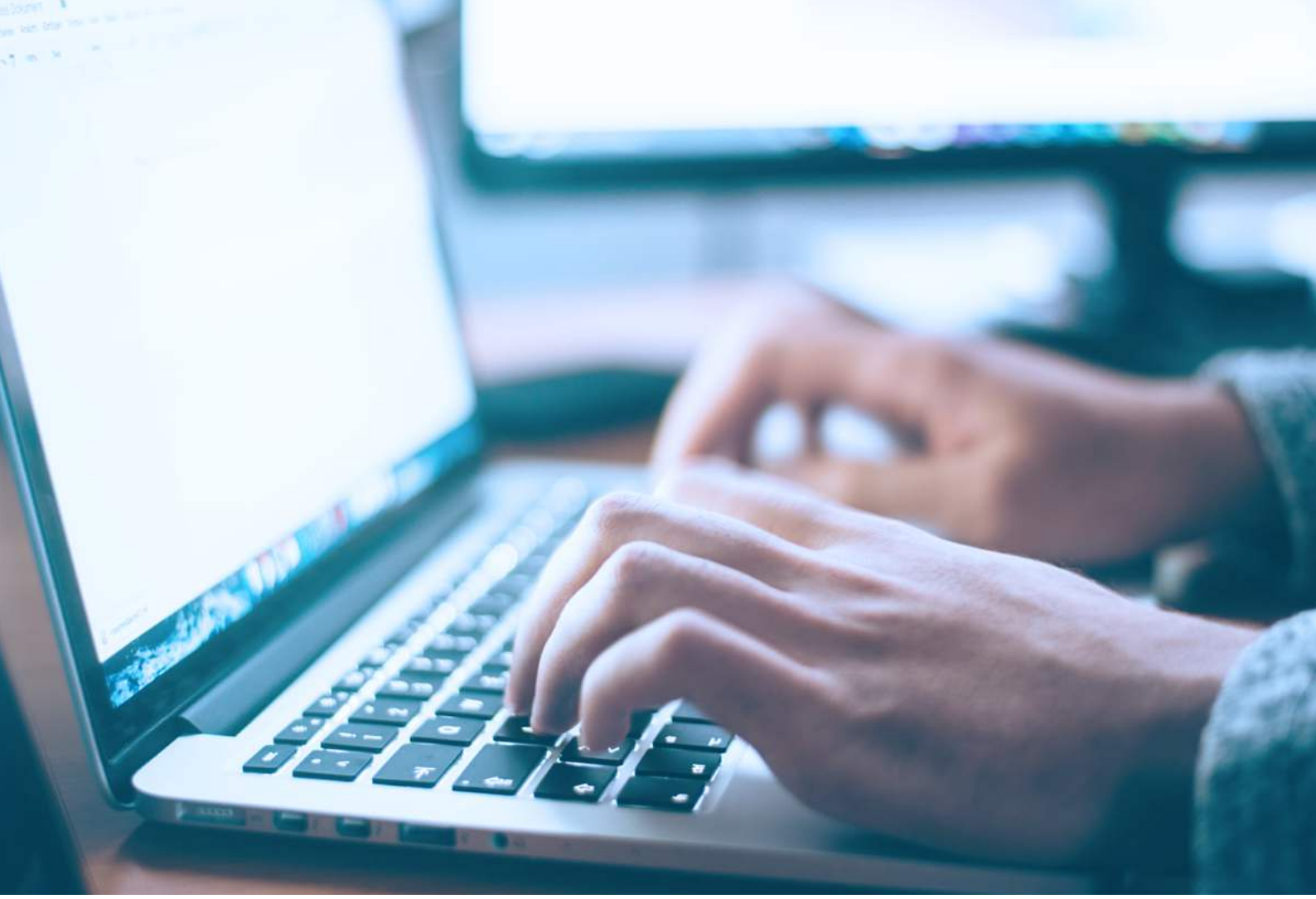
- Alastair MacGibbon – Chief Strategy Officer, CyberCX
- Jordan Newnham – Executive Director, Corporate Affairs, CyberCX
- Megan Lane – Director of Communications and Government Affairs, CyberCX
- Emma Dawson – Executive Director, Per Capita
- Shirley Jackson, Director, Centre for New Industry at Per Capita

# Introduction

Australia is experiencing a critical skills shortage across the Information and Communications Technology (ICT) sector, but the most significant skills shortage appears to be in the increasingly important Cyber Security sector. While this shortage is not necessarily unique to Australia, given the significant increase in workforce size and capability needed in the short and medium term, it is arguably a significant economic and national security concern. A major study of technical professionals and educators identified Cyber security as the most significant technical skill shortage globally (Pluralsight, 2022). This international contestation will result in competition for migrant talent within key markets where there is no dearth of talent.

While the number of students undertaking degrees and diplomas has grown in aggregate terms, the increase has not kept pace with the emerging needs of the sector, particularly as the increase in candidate numbers skews largely to international student enrolees. Addressing this skills shortage, given the highly technical nature of the work, is not possible through any singular approach. The nature of this shortage necessitates a co-ordinated approach, and one that includes a re-evaluation of the traditional approach to technical education.

Alternative approaches are needed to hasten our response to the existing and emerging skills shortages, involving greater investment in both existing learning pathways and emerging supplementary pathways. The tertiary sector continues to grow the talent pool but, given the technical and highly applied nature of many aspects of cyber security work, professional and practical experience is highly valuable. Supplementary models such as the increasingly popular bootcamp/intensive model and the cyber security firm based 'academy' model represent viable additions to the cyber security education framework.



These alternatives supplement the core vocational and higher education offerings, and support more rapid reskilling of individuals from different technical and non-technical fields. They are a viable supplement to, and articulation pathway from, existing vocational and tertiary programs.

Given the Australian Signals Directorate's critical REDSPICE initiative that seeks to dramatically increase Australia's cyber defence capability, the need for a significant increase in the size of the domestic talent pool is substantial. Crucially, there needs to be a particular emphasis placed on the technical capability that are necessary in a genuine shift away from the traditional *Linear Learning* approach to upskilling and reskilling to a more *Dialectic Learning* approach, that supports expedient movement between sources of skill-based training.

The report models the shortfall within the cyber security workforce, forecasting the anticipated increase in the size of the workforce needed by 2026. The report examines sector demographic and retirement trends, and technical requirements needed to contribute viably to the sector. The report then outlines an alternative approach to upskilling and reskilling, involving more expedient movement between. The report also considers the supplementary role of targeted migration in addressing technical skills shortages.

The Australian workforce possess the necessary talent to address the shortfall if adequate investment in upskilling and reskilling is made, while acknowledging he need for a targeted program of migration to supplement the investment in domestic capability.

# An Overview: the Cyber Security Workforce

At a time when cyber security, and the repeated digital attacks that try to subvert it, are front page news the capabilities and capacity of the workforce responsible for our protection becomes paramount. Presently there are approximately 68,400[1] cyber security professionals (including database monitoring and administration) within the Australian workforce (ANZSCO code 2621)[2]. While these workers are highly skilled and provide crucial support to Australia's businesses, public services and households, there is a strong consensus that this cohort is not sufficient to meet increasing market demand for cyber security services, and as such the sector is facing a significant skills shortage.

Data collected by the International Information System Security Certification Consortium (ISC)2® puts the current shortage at 25,000 professionals, while National Skills Commission (NSC) data indicates that we will need an additional 30,000 over the next four years to keep up with our rapidly changing security needs. It is notable that pre-2019 estimates and forecasts do not reflect the significant surge in cyber crime, and cyber risk more broadly, that is largely driven by the prolificacy of ransomware and data theft extortion.

Cyber security workforce shortages are becoming increasingly pronounced, as organisations across the private and public sectors are finding recruitment increasingly challenging within the sector, with only five applications on average for many listed opportunities, and only one in four applicants demonstrating the requisite skills to meet role expectations (ISACA, 2017).

While the tertiary sector is playing its part in the redress of skills shortages, no singular strategy can address the shortfall of candidates in isolation at a time of rapidly increasing demand.

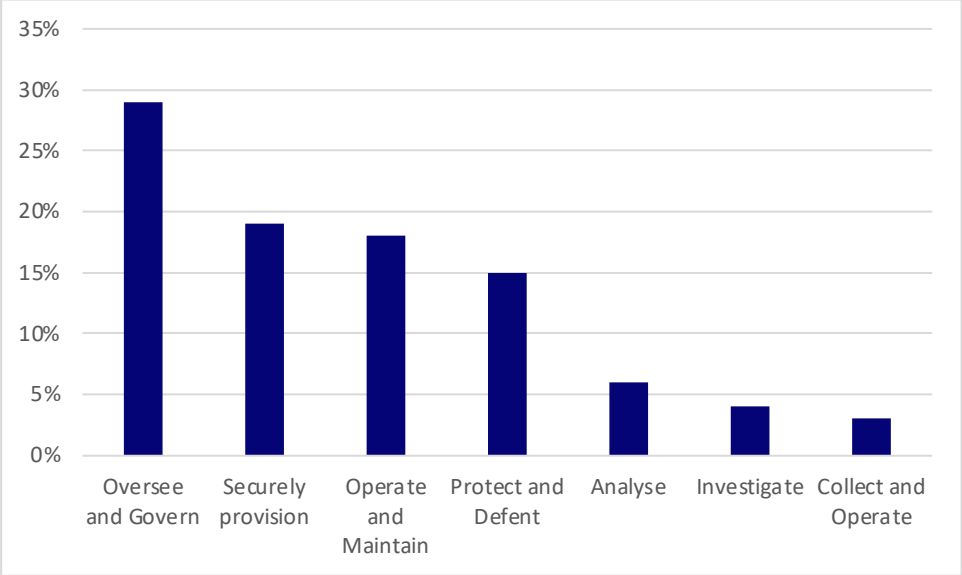
## Existing Cyber Security and ICT Sector Workforce Dynamics

Labour market analysis provided by the National Skills Commission offers worthwhile insight into the dynamics of the existing cyber security workforce. While most professionals work with systems or database administration, the specialisations across the sector are skewed towards the more oversight and governance focused roles, leaving key capability deficits unmet.

1 Within the highly specialist ICT security category there are an estimated 4,800 employees (ANZCO 262112). Research commissioned by AustCyber puts the figure at approximately 30,000, when employing a broader, albeit equally valid definition.

2 This category is substantially broader than ICT Security, noting that the other ANZSCO coded categories are broadly aligned to cyber security/security roles per the NICE classification. Also note that the IC3 Cyber security workforce study suggests a larger pool of 164,390, but a current shortage of 25,000 which by implication suggests a greater overall skills shortage than the National Skills Commission datasets.

Figure 1: Distribution of cyber security workers across role focus (Australia)




*Source:* (ISC)²® *(2021)*

The (ISC)²® study into cyber security offers detail into the specific skillsets of cyber security workforce. There is a strong preference or overrepresentation of governance and provisioning, with only modest numbers working within critical Protect and Defend, Analyse and Investigate roles. This data was reflected in the attitudes of qualitative participants in our research, who reported a skew towards non-technical capabilities and a weaker market for individuals with strong technical skills.

Additionally, there is a significant gender imbalance within the cyber security sector that is consistent with the broader gender imbalance across digital industries more generally. While women are 48 percent of the overall workforce, they make up only 21 percent of all staff employed within the cyber security and systems administration workforce, indicating a broad inequality in the technical and income distribution across the workforce.

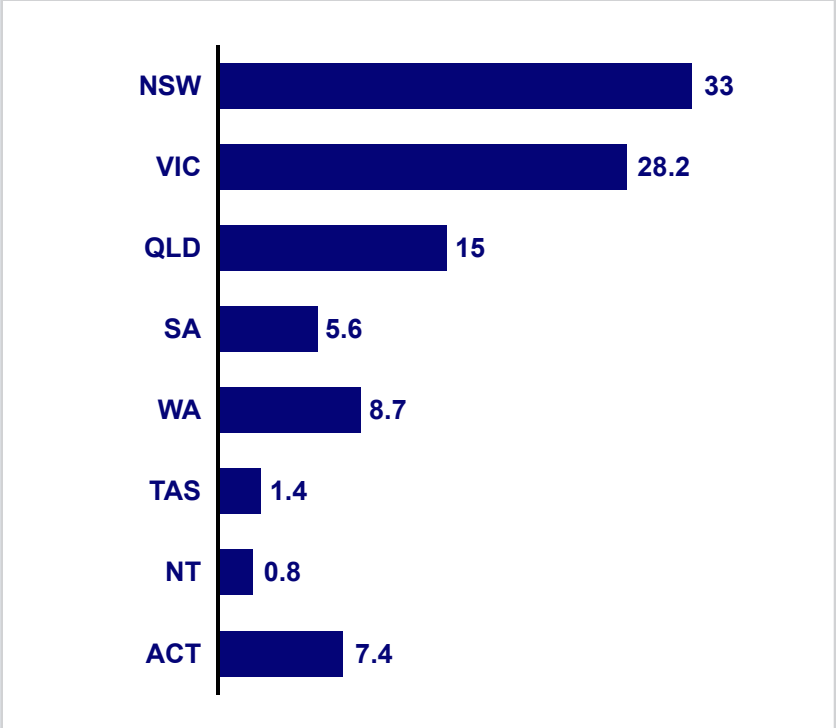
Figure 2: Gender distribution of cyber security workforce

*Source: National Skills Commission (2022)*

The sector is highly skilled with most professionals possessing an undergraduate degree. However, when we explored the need for undergraduate and postgraduate qualifications with the reference group, they noted that many cyber security roles did not necessarily require a university level qualification. While this assertion was dependent upon category and focus, TAFE and other vocational qualifications are viewed as being of significant worth and immense practical value.

The geographic distribution of workers in the sector is consistent with expectations reflecting population dynamics and attack frequencies broadly, but the data does suggest that greater capacity may need to be fostered in Western Australia, South Australia, the Northern Territory and Tasmania. The ACT is emerging as a critical cyber security hub and this should continue to be cultivated.

Figure 3: Cyber security talent distribution




*Source: National Skills Commission (2022), Per Capita (2022)*

The cyber security workforce is already a significant contributor to the economy, with recent research conducted as part of a digital census effort determining that the Gross Value Added by the sector is approximately $2.3 billion. The research identified that the sector value add is already comparable to other critical digital sectors such as computer software (approximately $4.2 billion) and retail e-commerce ($3.2 billion)[3].

3 For more information please refer to the AustCyber Digital Census 2021

## REDSPICE and National Security Workforce Dynamics

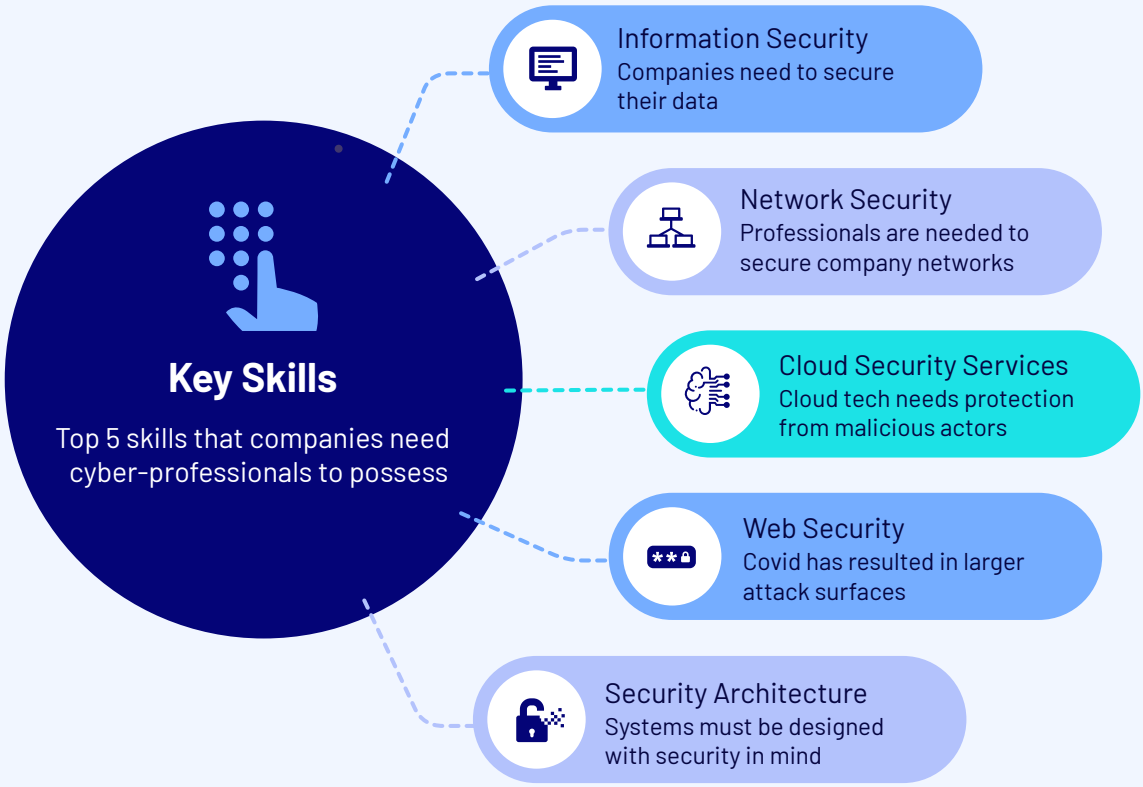
The national security community has experienced the cyber skills shortage alongside other parts of the Australian economy and cyber ecosystem, reflecting a broader deficit in our digital workforce. This has in part been driven by geographic constraints, and public sector pay scales, which can be less flexible than some of those offered by the private sector. However, in March 2022, the Australian government announced its largest ever commitment to cyber recruitment through its new REDSPICE program.

REDSPICE aims to recruit 1,900 technical professionals in the Australian Signals Directorate, of which a subset will be cyber security professionals in response to the deteriorating strategic landscape in the region.

## Cyber Security Sector Specific Skill Requirements

Before proceeding to the tertiary sector specific analysis, vocational sector analysis and forecasted workforce shortfalls, it is important to consider the skills and competencies necessary for success within the cyber security sector. Crucially, we must acknowledge that the sector is not homogenous and requires the participation of many diversly skilled individuals in order to thrive.

Figure 4: Most in demand skills within the cyber security workforce




*Source: Robert Half (2021), Per Capita (2022)*

While there are several critical skills that are in particular demand, there are many ecosystem needs beyond those noted in Figure 4. This is because of the diverse nature of ICT, the diversity of plausible modalities for cyber risk to be realised, the duality of cyber defence being both physical and digital, and the changing nature of attack surfaces.

Table 1: The 31 Cyber Security Specialties

| SECURELY PROVISION | PROTECT AND DEFEND |
|---|---|
| System Requirements Planning | Computer Network Defence Infrastructure and Support |
| System Development | Vulnerability Assessment and Management |
| Software Engineering | Incident Response |
| Enterprise Architecture | Computer Network Defence |
| Test and Evaluation | Security Program Management |
| Technology Demonstration | |
| Information Assurance Compliance | |
| **OPERATE AND MAINTAIN** | **INVESTIGATE** |
| System Administration | Investigation |
| Network Services | Digital Forensics |
| System Security Analysis | |
| Customer Service and Technical Support | |
| Data Administration | |
| Knowledge Management | |
| Information Systems Security Management | |
| **SUPPORT** | **OPERATE AND COLLECT** |
| Legal Advice and Advocacy | Collection Operation |
| Education and Training | Cyber Operation Planning |
| Strategic Planning and Policy Development | Cyber Operations |
| **ANALYSE** | |
| Cyber threat analysis | |
| Exploitation Analysis | |
| Targets | |
| All source intelligence | |

*Source: National Initiative for Cyber Security Education 2022*

The National Initiative for Cyber Security Education (NICE) lists a remarkable 31 primary level cyber security specialities, across seven groupings – Security Provision, Operate and Maintain, Operate and Collect, Protect and Defend, Investigate, Support and Analyse – highlighting the diversity of skills need with the sector. We explore the alignment of tertiary designations to the seven high level categorisations within our cyber security education sector mapping and analysis within the ensuing discussion.

# Cyber Training Pathways

## Analysis of Educational Pathways into Cyber Security Careers

As with other highly skilled career paths, several entry points and articulation pathways are necessary to ensure the viability of the cyber security sector: no singular model, whether vocational, tertiary, or accelerated non-traditional pathways (such as bootcamps, industry certifications or increasingly popular professional academy models) can address sectoral need in isolation.

However, more recent articulation pathways into professional services made possible by private cyber security firms are noteworthy and provide candidates with practical experience that makes such pathways worthwhile additions to traditional tertiary pathways. While tertiary pathways remain the cornerstone of industry training, the role of cyber firms and agencies in professional training should be appraised and suitably supported.

Per Capita conducted an extensive analysis of education providers, including TAFEs and universities delivering designations in cyber security. The analysis also explored emergent models such as the *Academy model* and *Intensive Graduate model*. The analysis suggests that there has been a significant increase in the number of university courses with named cyber security designations and cyber security majors since the most recent study predating Per Capita's analysis.

## University Pathways

Per Capita reviewed 199 undergraduate and postgraduate cyber security and ICT designations offered by 38 universities across Australia. Sector specific analyses were previously conducted by Caelli and Liu (2018); with the research identifying some modest progress in cyber security focused program design. Since 2018 there has been a significant increase in the number of qualifications in cyber security, particularly named cyber security qualifications.

There has been a dramatic shift in the modality of delivery, scope and focus of many of the qualifications traditionally offered by these institutions, with a significant increase in the number of dedicated cyber security specialisations. Currently, there are approximately 87 tertiary qualifications that are dedicated to ICT/cyber security (an increase from seven programs in 2018, Caelli & Liu (2018)), and a further 58 qualifications that offer a cyber security major. A further 54 qualifications did not incorporate cyber security majors, but did allow for the selection of cyber security subjects through, breadth and other student choice mechanisms. Notably most of these three-year programs have been established in the last couple of years, and consequently may take time to see significant uptake. The qualifications appear to be well specified and map to the critical domains of cyber security.

## TAFE Pathways

Crucially, in both tertiary and vocational system, cyber security qualifications were offered by all institutions reviewed, though the level of uptake of these qualifications remains consistent. A significant number of learners undertaking study in a digital qualification were not domestic candidates and consequently there remains significant potential for a reverse brain drain effect post completion, as international students qualify and repatriate to their countries of origin. Therefore, consideration must be given to mechanisms that incentivise the brightest and best learners to stay in Australia and contribute to the national economy.

Per Capita reviewed the ICT and cyber security qualifications offered by the major TAFE providers within each state, noting that all major TAFE providers offered qualifications in ICT/cyber security.

The qualifications with both the TAFE and University system appear well scoped, covering critical elements of the cyber security body of knowledge and generalist ICT technical skills. The emergence of several focused postgraduate qualifications is also a promising point of progress since 2017. These new degrees and diplomas offer a viable pathway for existing professionals to segue into cyber security.

TAFECyber is a notable initiative seeking to make the TAFE programs more relevant and accessible and promote the uptake of TAFE based cyber security initiatives.

## Graduate and Student Sentiment and Completion

Per Capita analysed data provided by the National Centre for Vocational Education Research (NCVER) to explore rates of satisfaction post completion and graduate outcomes. The analysis indicated that graduate satisfaction was high at 71.2%, and median salaries post completion were $57,400, with the 39% of graduates working in professional or technical services post completion (NCVER, 2021).

The analysis also identified only modest completion rates within the key fields of ICT and Engineering principal feeder courses for the ICT and cyber security sectors. The rates of completion suggest that greater promotion and advocacy that highlighted the benefits of qualifications within these categories would be highly beneficial.

TAFE qualifications in these categories are increasingly viable for individuals seeking a practical skillset, but uptake remains low, notwithstanding the government fee waivers provider by both state and federal governments. Further incentivisation by way of scholarship akin to those offered for the TAFE completion may be beneficial to the sector.

Government-supported marketing of the benefits of the vocational offerings and the sector specific need would benefit learners and institutions in the matching process, given that public awareness is presently perceived to be modest at best. There are several promising category specific initiatives that are part of the response to the workforce shortages.

# The Cyber Skills Crunch

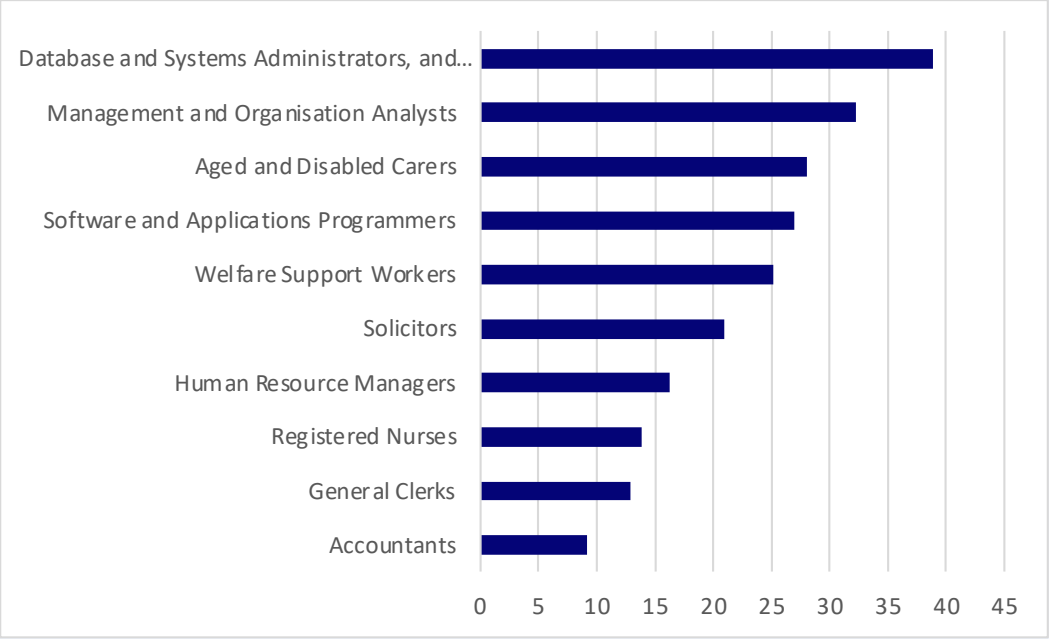
While several sectors are experiencing skills shortages, evidence suggests that the cyber security industry is experiencing the greatest difficulty in securing viable talent, with analysis determining that cyber security to be the technical skillset in shortest supply (Pluralsight, 2022).

Cyber security skills are now in shorter supply within the workforce than cloud computing and cloud infrastructure (the skill previously in shortest supply now ranking second to cyber security). Additionally, there is strong international contestation for cyber security talent, with many experienced cyber security professionals able to access gainful employment opportunities in more developed markets such as Canada, the UK and the US.

Research conducted independently by the Information Systems Audit and Control Association (ISACA) and Centre for Strategic and International Studies (CSIS) identifies that the greatest challenges are in the recruitment of technical talent. 52 per cent of the organizations surveyed said the biggest shortfall problems were in the area of technical staff, while 72 per cent said that they currently have no C-suite openings for cyber security management roles (ISACA, 2022).

When exploring workforce shortages in the Australian cyber security sector, database management and ICT security are considered amongst the most in demand skillsets. Indeed, the category is anticipated to present the most growth potential of all segments of the workforce.

Figure 5: Forecasted increase in workforce by ANZCO sub-category

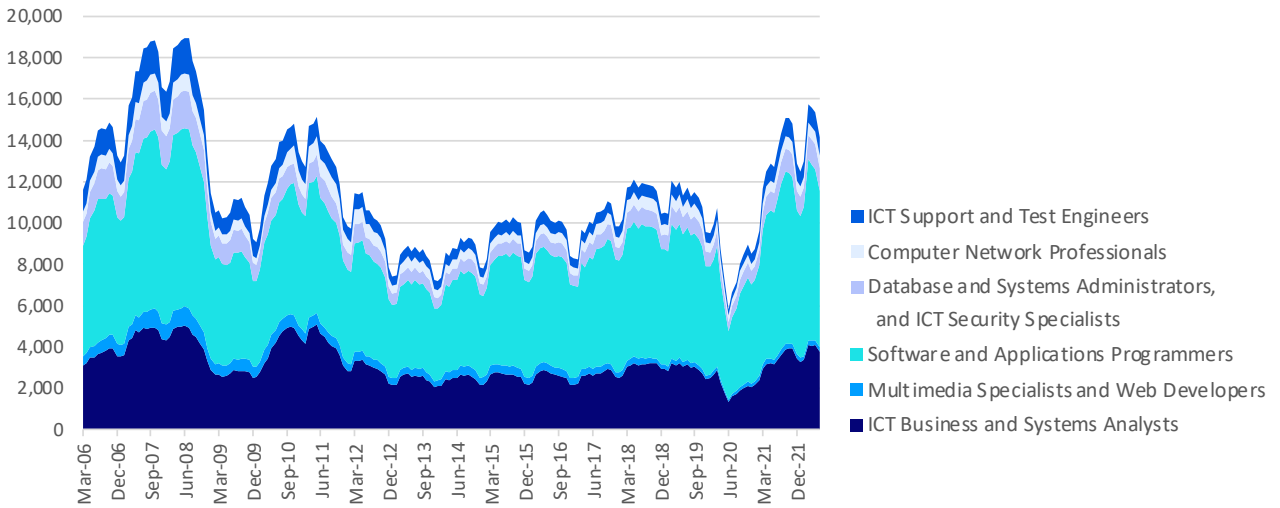



*Source: National Skills Commission (2022)*

The anticipated growth is estimated to be greater than 38 per cent, more than anticipated for the care sector or even software development, two burgeoning segments of Australia's workforce. As noted earlier in this report, the anticipated shortfall in cyber security sector professionals is estimated to be approaching between 25,000 ((ISC)$^{2®}$, 2020) to 30,000 (NSC,2022) professionals over the next three to four years.

Our discussions with domestic recruiters and members of the research reference group also reflected this disparity with a genuine shortfall of technically capable staff within the sector, and that this pattern is not dissimilar to the pattern observed within other jurisdictions.

Figure 6: Total ICT workforce demand




*Source: NSC (2022)*

Indeed, these shortfall estimates may understate demand given the significant elevation in the associated Internet Vacancy Index (herewith IV Index or IVI)[4] data pertaining to the category and associated categories. Recruitment numbers within the Database and Systems Administrators and ICT Security Specialists category have increased dramatically since the pre-COVID period.

Addressing this anticipated shortfall is going to be a genuine challenge. However, it is not insurmountable given the emergence of viable accelerated models of education (Academy/ Intensive graduate models), strong vocational pathways (CyberTAFE), and quality tertiary programs with a dedicated cyber security focus[5].

4 Demand data deriving from CareerOne, Seek, Australian Job Search.

5 Dr Tobias Feakin, often described as Australia's first "cyber ambassador", has noted that "The current shortfall in the workforce—and the research and development base which complements it—can only be fixed through investment in sound policy and a long-term education plan that targets high schools and universities to promote careers in the cyber security profession"

# Modelling the Workforce Shortfalls in Cyber Security and ICT

By virtue of the dearth of sector specific data in disaggregated form (that is cyber security workforce specific data with a specific subcategory focus) and given the generalist nature of many ICT qualifications currently offered by vocational and tertiary providers that provide scope for cyber security entry, this paper explores the broad sectoral need for graduates at an ICT sector level.

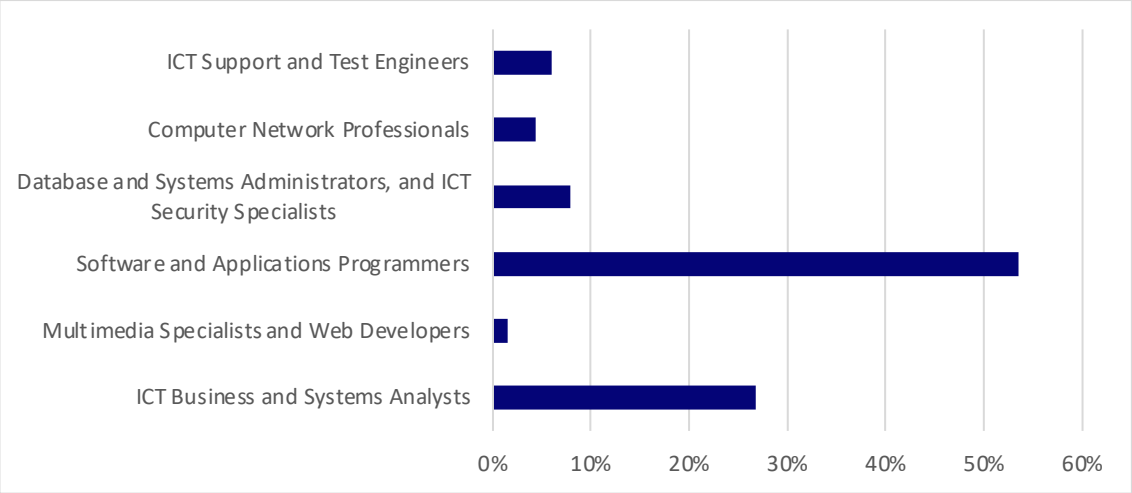
Employing some assumptions based on Job Index data, and NSC estimates, we can consider the capacity of the tertiary and vocational systems to supply category relevant talent, absent of engagement with Academy models and targeted programs of migration. We then consider cyber security sector specific needs employing shortfall estimates and cyber security talent 'draw' employing Job Index data[6].

As noted previously, domestic and international evidence put the current shortfall at 25,000-30,000 positions that will be needed by 2024. Both estimates appear to be derived soundly, with the NSC estimates based on ABS Labour Force Survey data.

We employ these estimates as our benchmarks when modelling vocational and tertiary system graduand rates in the first instance. We also note the additional domestic talent pool required to address the ASD REDSPICE initiative, the initiative of the ASD to dramatically increase Australia's sovereign cyber defence and security capabilities.

In the absence of granular data, we model overall technical talent pools derived from vocational/university programs across the ICT sector and then adjust the outputs based on subcategory employment demand data from the IVI.

Figure 7: Sub sector demand within ICT professional services




*Source: NSC (2022)*

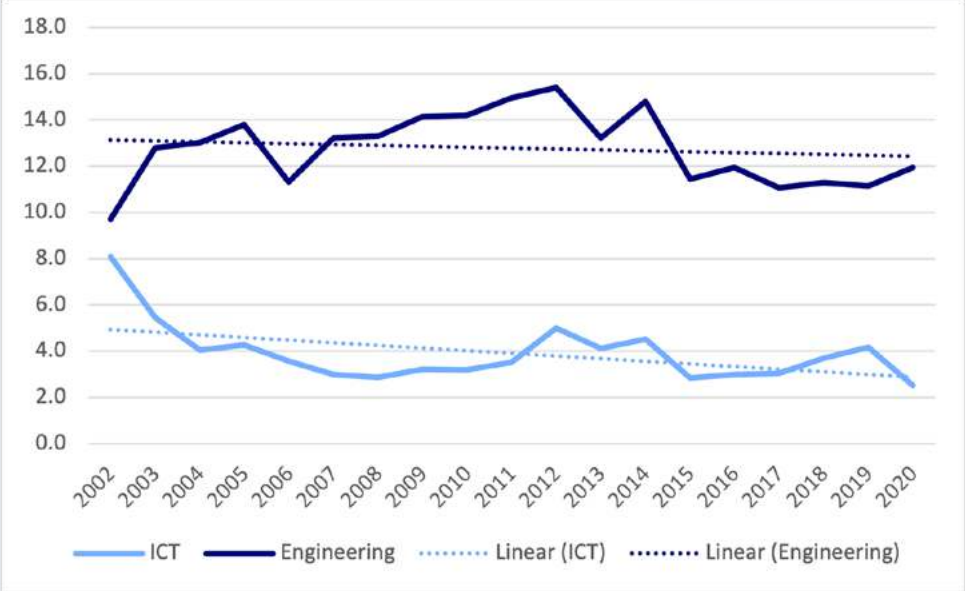
6 Given the significant association between Test Engineering/ICT Support and ICT Security for the Cyber security sector we may have been justified in apportioning the demand rate for test engineering; and then adding the apportioned rate to the ICT Security demand percentages; to determine the 'draw' (we employ this term to describe students drawn into the cyber security sector) rate of the cyber security sector on ICT/Computing graduates; with the remaining graduates deemed to be drawn to the broader ICT sector. There is a small degree of imprecision in this approach given the broad and overlapping nature of ICT roles, and it was deemed important for soundness of data alignment and conservatism in estimation, to align the specific ANZCO classifications.

# Trends in Completion Rates: TAFE

Per Capita explored the underlying trends in TAFE completion rates associated with ICT / Engineering certificates and diplomas, and ICT degree programs over the last two decades.

There are several notable observations deriving from the analyses. Firstly, when exploring TAFE completions data, there is a decline in ICT associated diploma completion rates. There is a similar, albeit more modest, decline in Engineering completion rates. There appears to be a recent countervailing trend whereby improved Engineering rates of completion are offset by a decline in ICT diploma completions. Given that the cyber security sector draws employees from these graduate cohorts the overall trends warrant attention.

Figure 8: TAFE completion rates within ICT and Engineering Courses

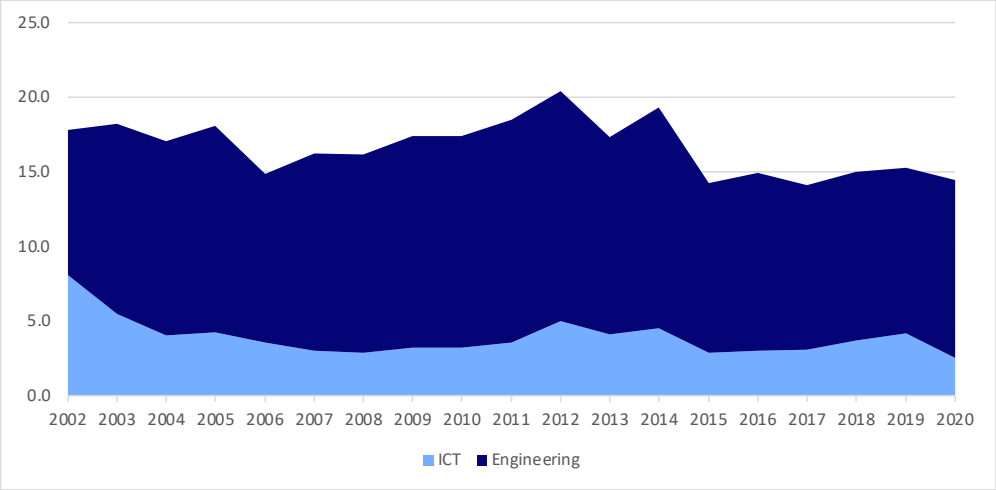



*Source: NCVER (2022)*

Overall uptake and completion rates in the TAFE sector, pertaining to ICT and Engineering, have been in decline since 2012, resulting in a smaller pool of vocationally trained professionals that are work ready.

This decline has coincided with elevated demand for ICT professionals. Again, for emphasis, this decline is most plausibly ascribed to a lack of awareness of the significant vocational opportunities, given the high quality of TAFE designations and strong quality indicators.

Figure 9: Total ICT completions in the TAFE sector (in thousands)

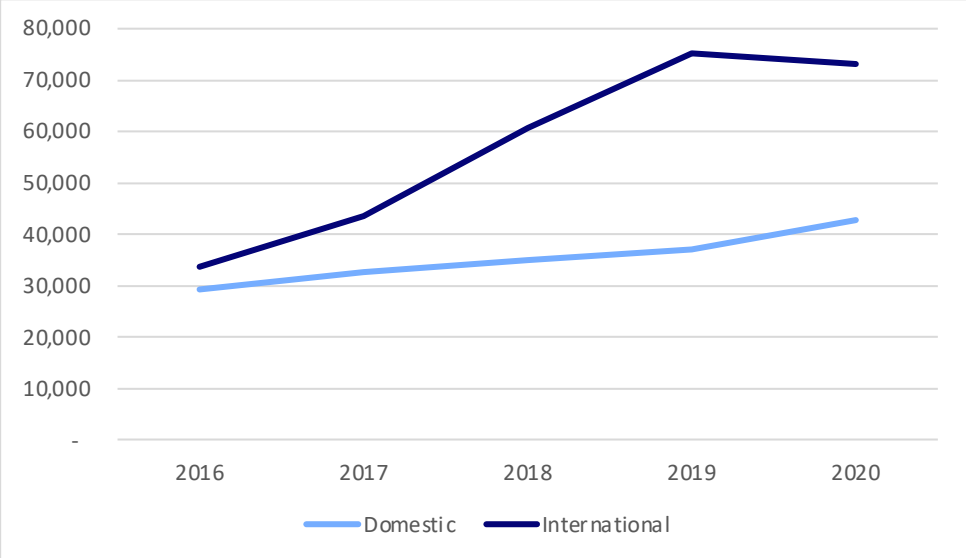



*Source: NCVER (2022)*

## Trends in Completion Rates: Universities

The trends within the university sector differ somewhat, showing modest increases in ICT associated enrolments.

Figure 10: Total ICT student completions in Australia at University level




*Source: DESE (2022)*

The number of enrolees continues to skew strongly to foreign enrolments. Across the tertiary sector attrition rates have been somewhat stable at approximately 14.2 percent of enrolees.

# Trends in Paid Employment and Sector Size Estimates

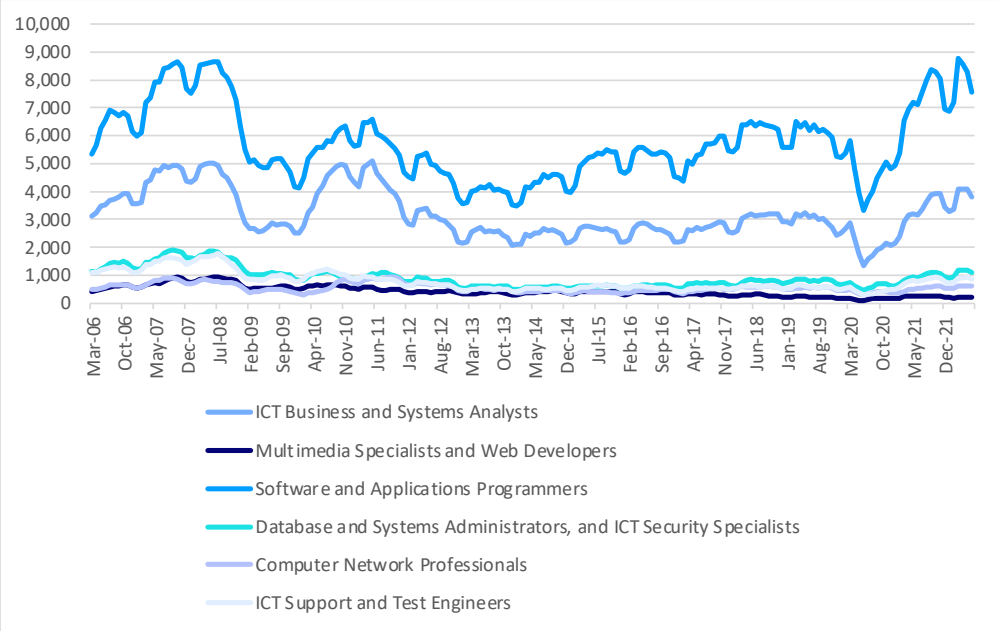
Estimates of sector size vary markedly largely due to differences in definitional scope, we employ NSC data and Australian and New Zealand Standard Classification of Occupations (ANZCO) vocational definitions for robustness and conservatism.

The trend in vocational opportunity is notable. Using data from the NSC IV Index, our analysis identifies an important post-2012 trend, with significant increases in all technical and ICT job listings. Further, listings pertaining to cyber security and associated disciplines account for approximately 7.90 percent of all ICT listings.

Even though there are greater skills shortages in cyber security than all other categories, other categories of ICT employment evidence strong workforce demand. There is significant contestation for cyber security and ICT talent broadly across all sectors of the economy.

Employing current job market indicators to determine the graduate 'draw' (we employ this term to describe students drawn into each sector) of each category, we determine plausible category specific uptake of future graduates, which ICT categories graduates are likely to work within.

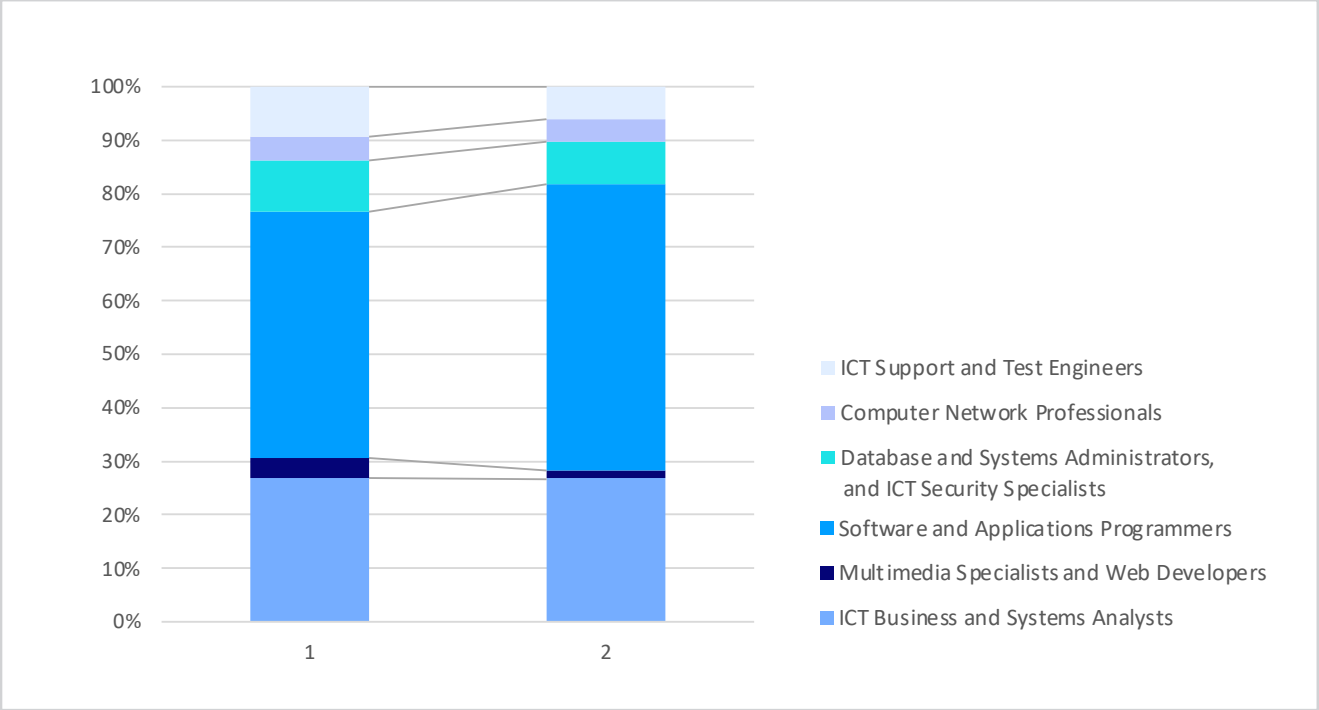
Figure 11: Internet vacancy index data for the ICT sector




*Source: IVI data/National Skills Commission (2022)*

It is anticipated that most ICT graduates will be drawn into programming and application development. The potential draw of candidates to cyber security is estimated to be substantially lower. The security segment and network professionals segments appear to be afflicted by some degree of crowding out caused by popular professions (ICT/Systems Analysts/Software/Applications programming).

Figure 12: Changes in ICT employment opportunities




*Source: National Skills Commission (2022)*

When accounting for category specific 'draw' and current graduate cohort numbers, we can estimate the candidate cohorts' potential future alignment. Employing sector specific demographic data, we can determine a plausible rate of retirement from the sector.

We note that the most logical approach for any learner would be to survey the market forecasts at the time of enrolment to determine the opportunity that presents the most significant scope for gainful employment.

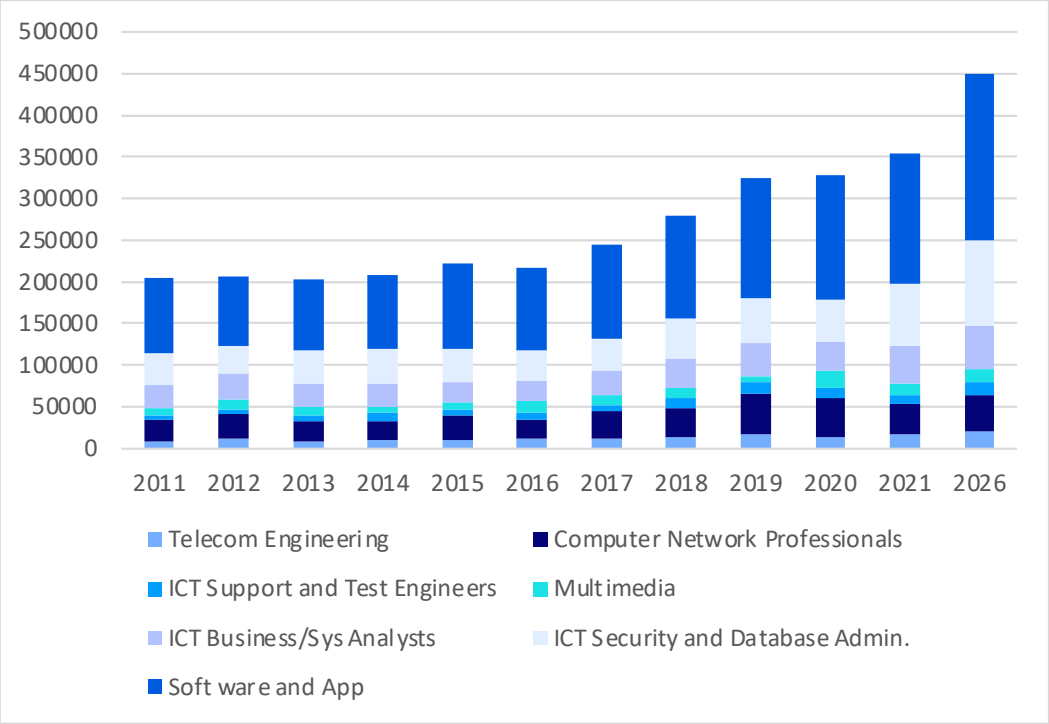
However, learners may not have access to perfect information, and employ current jobs data and sector size data to determine preferences. Similarly, learners may favour more established and longstanding professions and categories over less-established categories. There is a significant body of research pertaining to this decision process (see inter alia, Kori, 2015), and our indexation method is broadly aligned with the extant motivations research.

# Estimating the Graduate Cohorts and Sector Attrition Effects

Per Capita analysed the sector specific future workforce estimates and rates of attrition and retirement, to derive an estimate of the overall change in workforce size.

The ANZCO category classifications for ICT security and associated work categories present a forecasted increase in ICT demand of 95,000 by 2025.

Figure 13: Current and forecasted workforce size ICT sector



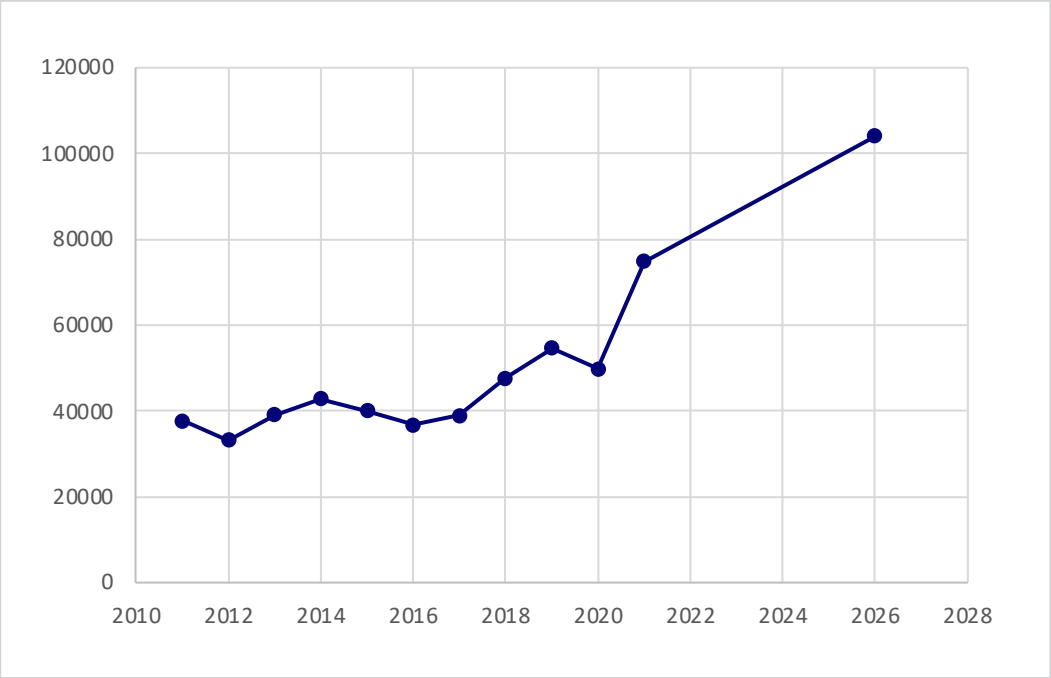

*Source: National skills commission (2022)*

This figure accounts for the anticipated change in the workforce size accounting for the seven ANZCO categories (4-digit code level). The figure does not account for industry attrition due to demographics.

When accounting for demographic factors and forecasted retirement rates, we estimate the additional number of cyber security professionals required is 124,727.

In the simplest sense this figure represents the number of new professionals that will be needed to meet workforce expectations. The most significant increase is anticipated (or required) in the ICT/cyber security/system administrator sector. The anticipated increase within this category is 29,200 between 2021 and 2025 alone, before attrition due to retirement.

Figure 14: Cyber security workforce size, current and forecasted



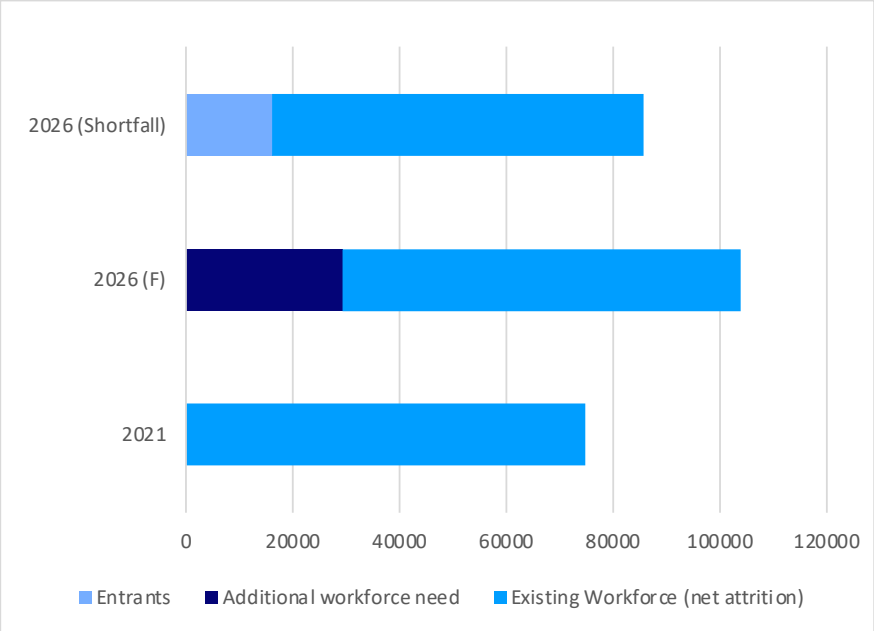

*Source: NSC (2022)*

To determine the number of candidates entering the sector we employ current TAFE and university entrant, and completion data and legacy attrition rates. We model contestation for talent across all categories of ICT employment, based on current IVI data (NSC, 2022) pertaining to employment opportunities.

The estimation approach is conservative and does not account for career shifting into non-ICT disciplines. We estimate approximately 16,184 entering the cyber security workforce over the next four years through tertiary pathways. Given the existing workforce and demographic factors, attrition/retirement patterns we anticipate a further 5,236 employees in addition to the increase in employees associated with the NSC forecasted change in employment level. A further 1,900 employees will be required to meet the requirements of the REDSPICE initiative.

Consequently, we anticipate a potential shortfall of 18,252 cyber security professionals (see Figure 15) in 2026, notwithstanding the current shortfall of 25,000 professionals asserted by (ISC)$^{2®}$. Were the current shortfall to be accepted, the overall sector shortfall in 2026 may approach the sum of the two figures.

Figure 15: Cyber security forecasted workforce requirement and forecasted shortfall




*Source: NSC (2022)*

Critical to addressing this skills shortage is an acknowledgment that there is a need for retraining and re-skilling, with a refreshed approach to transitioning learners and graduates into programs that enable them to gain the practical skills to perform well within the cyber security sector.

## Graduate Outcomes, and Upskilling/Reskilling opportunities

Some ICT graduates and graduates within other technical and non-technical categories are anticipated to be open to reskilling, given both the opportunity presented in economic terms, the apparent job security, and the compelling nature of the work.

Discussions with industry representatives evidenced an increasing number of cyber security professionals being recruited and retrained from other disciplines through intensive retraining and academy models.

This is evident when considering plausible skills overlap with other disciplines. Computer programmers, multimedia developers, and systems analysts all possess strong technical foundations, an understanding of modern digital technologies, and a rudimentary understanding of category specific exposure and vulnerabilities. Any unemployment of individuals from within these categories that is not driven by short-term market frictions could be addressed in part by a program of training with a Cyber Academy provider that is able to offer strong career pathways and potential term-based job guarantees, or through an alternative intensive retraining model.

Improving graduate pathways, particularly for TAFE graduates, to cyber security academy models is highly attractive.

Presently a significant number of technical graduates from the TAFE system, particularly in ICT, are working in non-technical professions, with retail ranking amongst the highest outcome professions for TAFE ICT graduates. These learners have received exemplary education within the TAFE framework and could find pathways into emerging Academy/Intensive training models provided by cyber security firms, into university courses in cyber security and into direct gainful employment opportunities within the category. Investment in these critical pathways is necessary to address the workforce shortages within cyber security.

# Solving the Cyber Skills Shortage

## Overview: The Role of TAFE

A refreshed model of cyber security education would see the TAFE system as a more viable entry point and pathway into professional services within the sector. The TAFE system would also be a viable mechanism for matriculation into the university system or intensive/academy models to allow for further supplementation and upskilling opportunities.

Currently a significant number of TAFE ICT/ Cyber security graduates do not enter the workforce as cyber security professionals. This is not because of a lack of quality in the education system, but rather a co-ordination and matching challenge. Some learners may also benefit from further intensive 'speciality specific' cyber security training to facilitate market entry. Intensive training and Academy pathways present as a viable market readiness upskilling opportunity for many learners.

Investing in domestic skill development in the TAFE sector is essential, but equally pertinent is the need to establish a more dynamic model of transition from the TAFE program to professional learning and/or gainful employment.

The TAFECyber consortium is an excellent initiative, with immense promise in facilitating better pathways. Further investment in embedded partnerships between TAFE providers and Australian cyber security entities and facilitation of access to Academy professional education is also essential.

## Overview: The Role of the Universities

The tertiary education sector is well placed to advance critical cyber security research in the national interest, as is the national science agency and CSIRO. There are only a small number of universities with Australian Research Council-aligned centres that have a cyber security focus. Positively, other universities have established their own research groups and centres to advance cyber security research.

Per Capita's research suggest that there are now over 18 university-based centres providing thought leadership and shaping cyber security education. These critical research groups are now at the forefront of cyber security education within the tertiary system.

These groups are critical to meeting the goals of the ASD and REDSPICE in particular, in providing a viable pool of professional capable of leading the cyber defence programs of the future. Consequently, funding for the academic programs they auspice, and the critical, practically focused research they lead is essential. Equally critical is fostering sound relationships and associations between leading Australian cyber security firms and these research communities to foster a research agenda that is rigorous and in the national interest.

# Overview: The Role of the Private Sector-Sponsored Academies

The emergence of the Academy model is also highly promising.

The model is akin to the traditional traineeship or cadetship model popularised in accounting and engineering. This model involves a private firm, often a cyber security advisory group placing a learner within the group, providing them with practical skills training and development opportunities.

Such programs have the benefits of providing the learner with a direct path to employment and industry relevant skills from the point of commencement. Per Capita reviewed Academy and Professional practicum models offered by a number of leading cyber security firms to consider the scope and focus of the programs and their context and relevance to the sector.

## Change the Learning Model: Linear to Dialectic

Current models of education show a linear path that is broadly inefficient for the purposes of upskilling. We find that a less linear approach to promoting the sector, and indeed promoting a greater uptake of qualifications through existing and emerging models, may necessitate a more fluid approach to achieving better learning and sectoral outcomes.

The more viable approach would see more fluid movement and articulation between segments of the educational system supporting cyber security professionals. Each segment serves as a viable entry point for school leavers, as well as a direct pathway for a graduate.

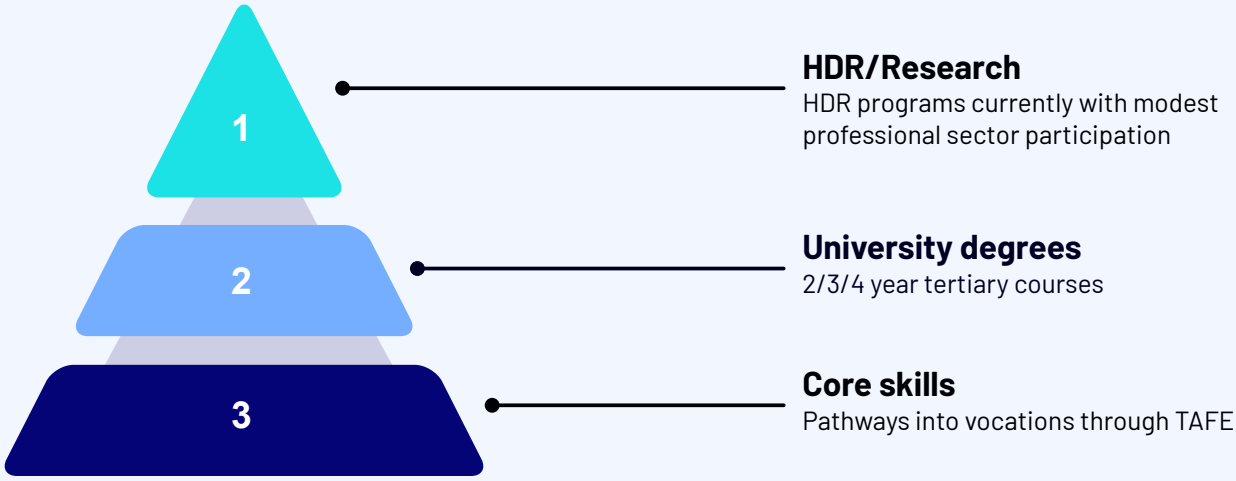
For example, it is envisaged that a school leaver could enter the TAFE system and then transition into an academy model, to access practical skills training, and expedite market entry. Alternatively, they could transition into university-based programs, or complete dual award programs. This flexibility allows for more rapid upskilling to meet the needs of the workforce. Similarly, school leavers should be able to enter intensive training through academies and then pursue gainful employment or transition into the tertiary system for further learning.

Alternatively, a non-technical university graduate could complete practical skills training through an academy model or intensive training program to access employment opportunities within the cyber security sector. This flexibility will allow non cyber security students to access gainful employment opportunities within the sector and address this critical skills shortage.

We describe this shift in approach as a shift from *Linear Learning* to *Dialectic Learning* which sees more movement between educational models. Linear progressions lock learners into defined paths and prevent rapid reskilling. By investing in dialectic model, all institutions benefit. Universities benefit from more work ready entrants, and from practically orientated research deriving from partnerships with academies. Under this model, TAFE institutions will be able to better establish themselves as viable paths to gainful employment and rapid upskilling to provide limited employment guarantees.

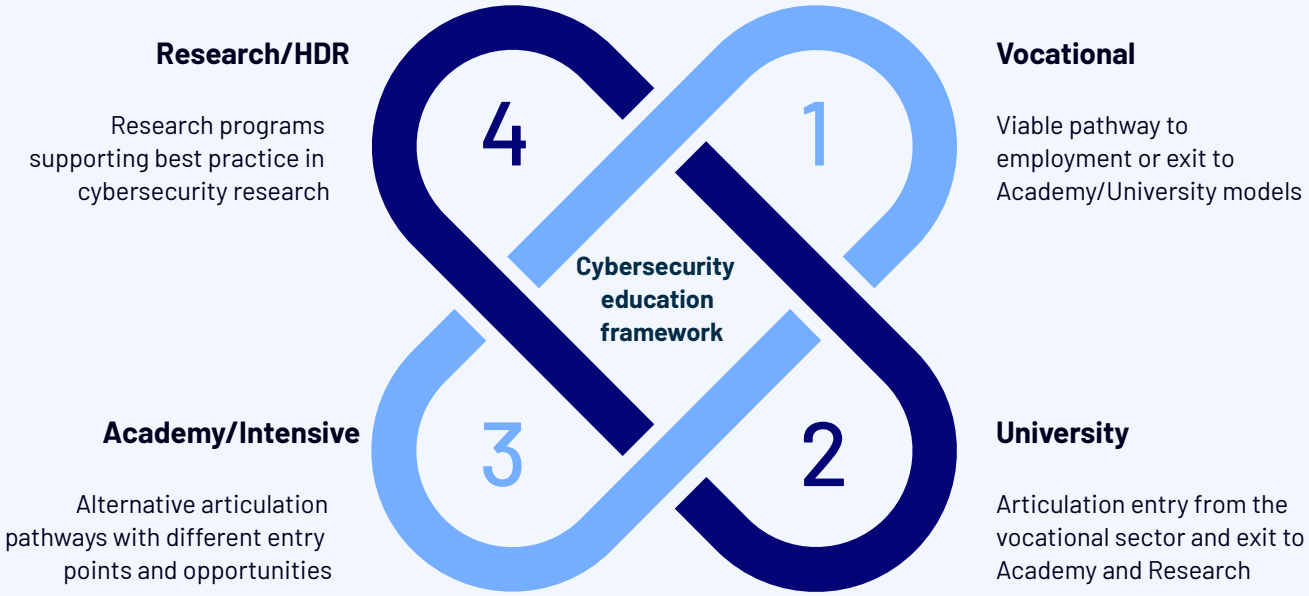
Academies would benefit through establishing more established pathways to and from traditional learning institutions, to procure and identify talent to meet the needs of Australian businesses seeking cyber security consulting support. These Linear and Dialectic approaches to cyber security education are illustrated in Figure 16 and Figure 17.

Figure 16: The Legacy (Linear) Model of Education in Cyber security

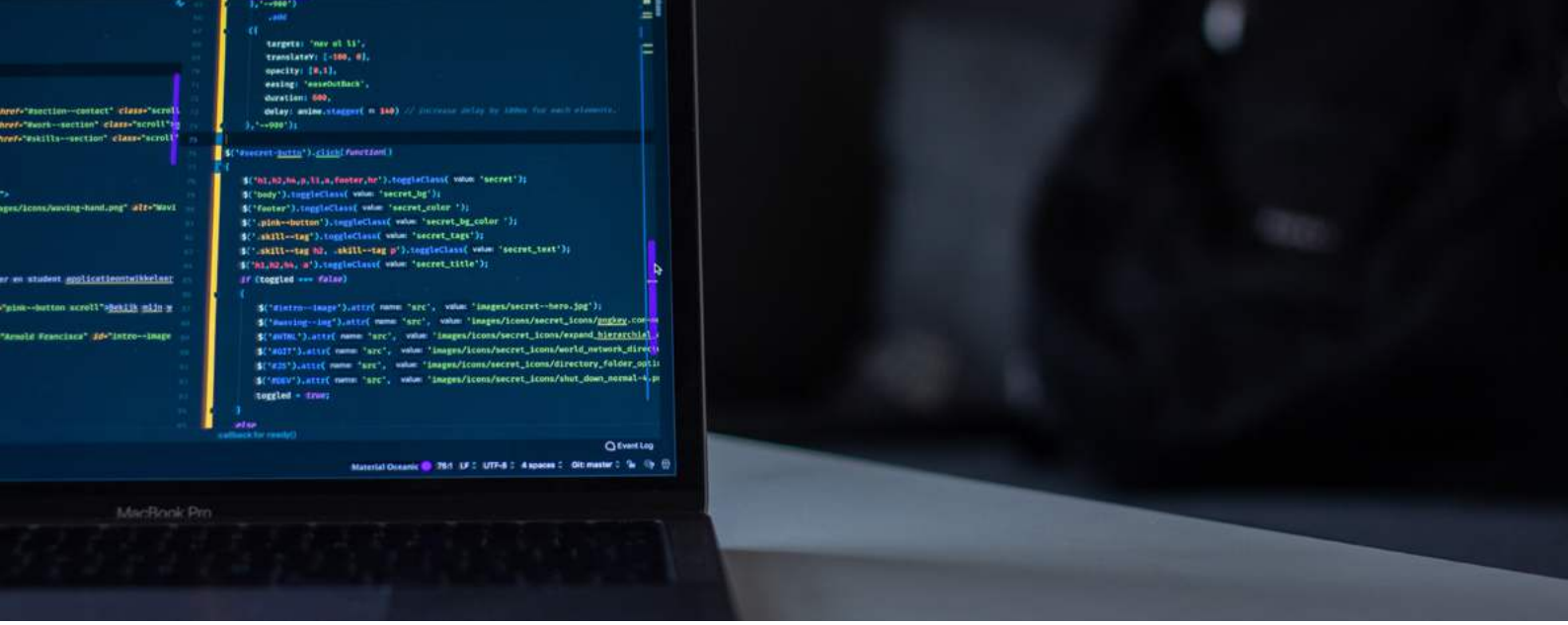



*Source: Per Capita (2022)*

Figure 17: An alternative (Dialectic) Cyber security education framework




*Source: Per Capita 2022*



## Migration in the Mix

The established shortfall of suitable qualified and capable professionals has dramatic implications for our national security and the ability of Australia firms to protect themselves from the ever-expanding array and volume of cyber attacks.

Additionally, the pandemic has seen many prospective entrants to the sector return to their country of origin as part of a 'reverse brain drain'. The reasons for their departure differ markedly, some due to visa associated issues, other student professionals because of financial constraints.

While a discussion on domestic investment in skills and training is vital, as emphasised no strategy to address the cyber skills crunch may be employed in isolation.

What is most important in response to the skills shortage is the implementation of a co-ordinated strategy involving all critical stakeholders from the knowledge sector, government and the private cyber security sector. A viable response will involve the use of targeted migration to supplement any critical shortages in the short term to ensure the viability of the critical ecosystem.

The role of migration in responding to the sector specific shortages should not be disavowed, particularly noting that migration and investment in skills and the foundational economy are not mutually exclusive. While such opportunities are often presented in a dichotomous manner, they are actually highly complementary, particularly with regard to the strengthening of the research and innovation base within the cyber security sector. Securing top tier cyber security talent will enable cyber security firms to offer recent graduates strong support, guidance and tutelage.

Category-specific targeted migration should not be at the expense of investment in the foundational economy and the local talent pool, but it is a critical supplement. The current skilled migration program strongly supports the migration of cyber talent (see Table 4), and this may be necessary in the short term as the sector continues to face workforce shortages. More expedient and longer term Visa categories may be necessary in the short to medium term, depending on cyber crime rates and changing business requirements observed over the coming months.

Table 2: ICT Security Specialist (Visa categories)

| | |
|---|---|
| **186** | Employer Nomination Scheme visa (subclass 186) |
| **189** | Skilled Independent (subclass 189) - Points-Tested |
| **190** | Skilled Nominated (subclass 190) |
| **407** | Training visa (subclass 407) |
| **485** | Temporary Graduate (subclass 485) - Graduate Work |
| **489** | Skilled Regional (Provisional) visa (subclass 489) - Family sponsored |
| **489** | Skilled Regional (Provisional) visa (subclass 489) - State or Territory nominated |
| **482** | Temporary Skill Shortage (subclass 482) – Medium Term Stream |
| **187** | Regional Sponsor Migration Scheme (subclass 187) |
| **494** | Skilled Employer Sponsored Regional (provisional) (subclass 494) - Employer sponsored stream |
| **491** | Skilled Work Regional (provisional) visa (subclass 491) State or Territory nominated |
| **491** | Skilled Work Regional (provisional) visa (subclass 491) Family Sponsored |

*Source: Priority migration skilled occupation list*

It is critical however that any skilled migrants that are making valuable contributions to the Australian economy are retained, and employed securely, or there is significant risk of a reverse brain drain, whereby cyber professionals hone their skills within the Australian market but return after they have improved their capability set. Retention is critical to addressing workforce shortages and ensuring that skills are not lost in the increasingly contested international market for cyber security talent.

The Global Talent Visa Program is a significant and compelling initiative but given the existing quotas the program offers limited scope to address the current and future sector specific skills shortages in isolation. Presently the expedited visa program is targeting ten broad employment categories, and a significant number of associated subcategories, and consequently there are likely to be significant crowding out effects between sectors and industries.

# Recommendations

## Recommendation 1: Dialectic Learning and Pathways

Investment is made in alternative articulation and progression pathways with particular regard given to the emerging role of Academies and TAFE institutions in rapidly upskilling the workforce, while providing direct pathways to gainful employment and/or further tertiary study.

## Recommendation 2: Integrating TAFE and University Qualifications

Dual award universities and universities with TAFE articulation partnerships are supported in the delivery of dual award designations (Degree/Diploma), to enable learners to access gainful employment opportunities while completing articulation to degree programs.

## Recommendation 3: Investment in Academy Learning Models

Essential funding is vested with prospective Academy entities/programs that are subsumed within Tier 1 and Tier 2 cyber security consulting firms, that possess the internal capacity and capability to support learners through practical and experiential learning.

## Recommendation 4: Skilled Migration

That the need for a target skilled migration program to supplement investment in domestic capability is acknowledged, and that a suitable process is enacted to 'fast track' viable candidates into the Australian sector. Investment in targeted marketing within markets where there is no skills dearth in the cyber security workforce is necessary to accelerate the process, particularly given the departures that occurred because of the pandemic.

## Recommendation 5: The National Security Cyber Workforce

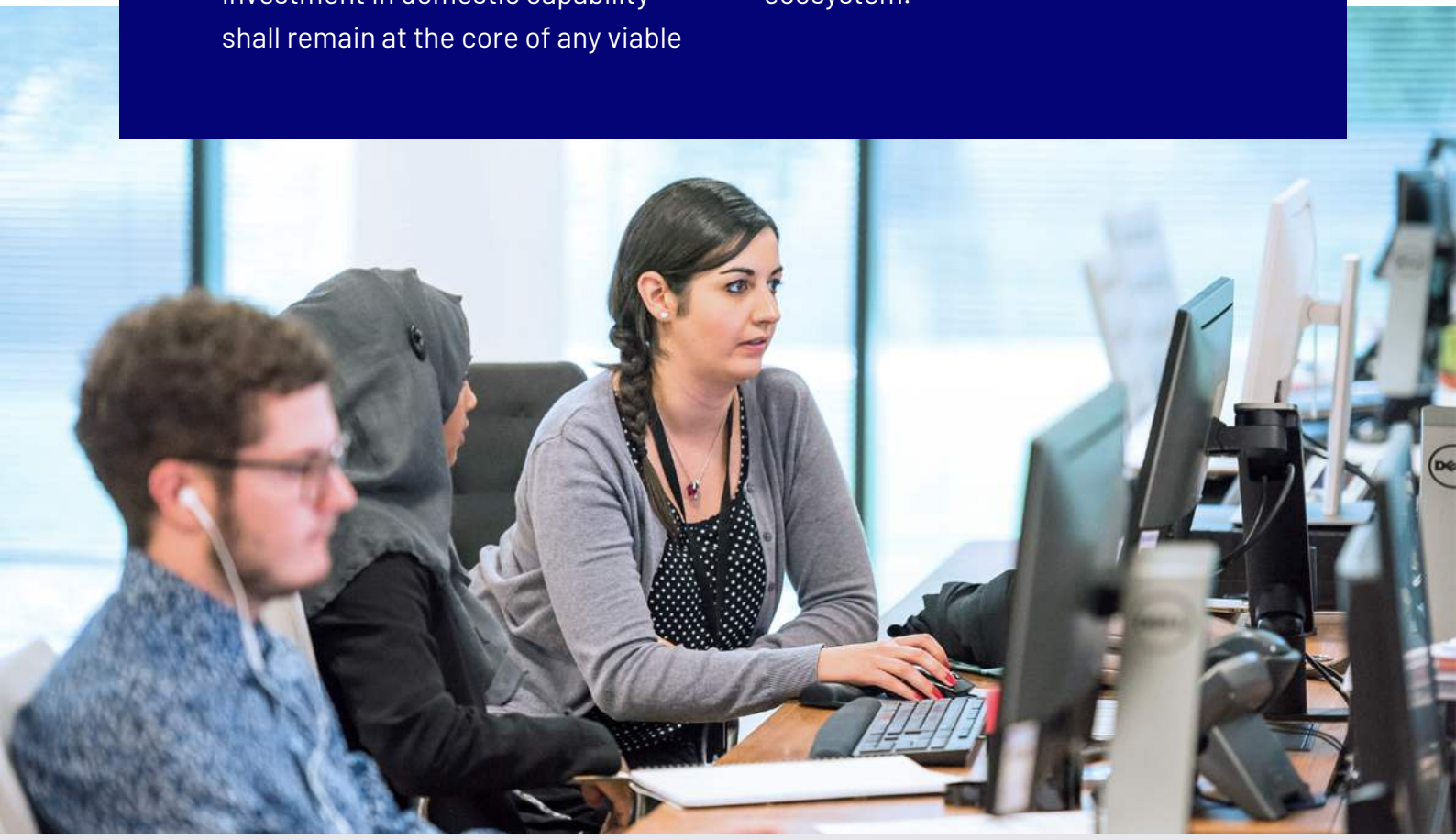
That Australia invests in national cyber defence capability through investment in domestic upskilling through funded training and upskilling for public sector workers. This is achieved through dedicated tertiary and vocational/academy partnerships. Given the sensitive nature of much of this category of work, establishing a domestic talent pool is essential to the national interest.

# Conclusion

These emergent models are highly flexible supplementary approaches that will be necessary to facilitate technical upskilling and reskilling of competent professionals from proximate or potentially unrelated disciplines seeking to contribute to the sector.

The role of a targeted program of migration that seeks to secure viable cyber security talent from markets not evidencing shortages, will also be necessary to supplement investment in domestic skills and capability. While investment in domestic capability shall remain at the core of any viable response to the skills shortage, it is evident that investment in domestic capability alone will not be sufficient to address all sector specific needs.

It is essential that all stakeholders remember what is at stake. Australia's critical infrastructure and essential systems rely upon this essential sector, which in turn relies upon this talent pool. With a renewed focus and adequate sector relevant investment in a refreshed approach to cyber security education we remain well positioned to meet the needs of this critical ecosystem.



# Appendix 1

## Analysis of sector specific recruitment challenges and prospective 'crowding out' effects

While workforce opportunities for Database and Systems Administrators, and ICT Security Specialists (for emphasis these roles fall within the cyber security role definition) are anticipated to increase more rapidly than any other profession, it is important to acknowledge that there appear to be shortages within every ICT category and profession that may be resulting in some crowding out effects, or shifting behaviours that may be deleterious to all IT sub sectors in the long term.

While Database and Systems Administrators and ICT Security Specialists are the fasted growing segment, the expansion of the Business and Systems Analysis, and Programmers category (herewith Programmers) is marginally greater in absolute headcount terms. So while ICT Security is the fastest growing, the Programmers category will need to add the largest number of employees to address shortages per skills priority list findings (ANZSCO sub-major group 26). As noted by the NSC, "of the Minor Groups, Business and Systems Analysts, and Programmers had the greatest proportion of occupations in shortage (38%), followed by Database and Systems Administrators, and ICT Security Specialists (33%)."

Moreover, unlike most professions that are anticipating modest future demand, 89% of all IT Professions anticipate strong demand (only 33% of all professions anticipate strong demand). NSC reports that:

> *The fill rate for ICT Professional occupations is primarily in the 60%-69% range, with close to three quarters of all occupations in this group in this range. Business and Systems Analysis, and Programmers was the only Sub-Major Group to have any occupations in the higher predicted fill rate range of 80%-89%.*

Regarding candidate viability, only 20% of candidate applications between 2020 and 2021 were deemed of viability. NSC note that:

> *The most common reason ICT Professionals were found unsuitable was due to a lack of either general or specialised experience in the occupation (both mentioned by around 60% of employers), followed by a poor application or poor performance throughout the recruitment process (mentioned by nearly 40% of employers). Employers of ICT Professionals valued experience over qualifications, with the vast majority (92%) of employers requiring applicants to be experienced in the occupation, compared with two thirds of employers who required applicants to have a qualification. On average, employers sought applicants with just over three years of experience.*

The data suggests that there is a concern about both candidate numbers and suitability. Moreover, given shortages within several priority skills categories there may be some candidate crowding out occurring, whereby high-quality candidates are suitable for roles across several ANZSCO codes, and firms are competing to gain the best talent. This may result in significant premiums being paid to lure top tier talent with the flow on effect being greater costs of service for ICT and Cyber security clients. Incentives may also serve to destabilise the emerging ICT categories and firms with individuals able to garner large premiums to move after short terms in the industry.

# References


ABS, Australian Bureau of Statistics Workforce Survey Datasets (2022)

ACSC, Australian Cyber Security Centre Datasets (2022)

Anderson, R., Barton, C., Bölme, R., Clayton, R., Ganán, C., Grasso, T., Levi, M., Moore, T. and Vasek, M., 2019. Measuring the changing cost of cyber crime.

Bada, M., Sasse, A.M. & Nurse, J. R. C. (2015) Cyber Security Awareness Campaigns: Why do they fail to change behaviour?, in proceedings of the International Conference on Cyber Security for Sustainable Society (CSSS) Coventry, UK, 118- 131.

Broadhurst, R. (2006a). Content cyber crimes: Criminality and censorship in Asia. Indian Journal of Criminology, 34(1&2), 11-30.

Broadhurst, R. (2006b). Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies and Management, 29(3), 408-433.

Broadhurst, R. and Kim Kwang Raymond, Choo, 2011. Cyber crime and on-line safety in cyberspace. in Smith C., Zhang, S. & R. Barbaret [eds.]. International Handbook of Criminology, Routledge: New York, pp 153-165

Broadhurst, R., 2006. Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies & Management.

Broadhurst, R., Grabosky, P., Alazab, M. and Bouhours, B., 2013. Organizations and cyber crime. Available at SSRN 2345525.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B. and Chon, S., 2014. An analysis of the nature of groups engaged in cyber crime. An analysis of the nature of groups engaged in cyber crime, International Journal of Cyber Criminology, 8(1), pp.1-20.

Burrows, J., Anderson, S., Bamfield, J., Hopkins, M. & Ingram, D. 1999, Counting the Cost: Crime against Business in Scotland, Scottish Executive, Central Research Unit, Edinburgh. Burrows, J., Tarling, R., Mackie, A., Lewis, R. & Taylor, G. 2000, Review of Police Forces' Crime Recording Practices, Home Office Research Study No. 204, Home Office, London.

Cabaj, K., Kotulski, Z., Księżopolski, B. and Mazurczyk, W., 2018. Cyber security: trends, issues, and challenges. EURASIP Journal on Information Security, 2018(1), pp.1-3.

Caelli, B. and Liu, V., 2018. Cyber security education at formal university level: An Australian perspective. In The Journal for the Colloquium for Information Systems Security Education (CISSE) (Vol. 5, No. 2, pp. 1-18). The Colloquium for Information Systems Security Education (CISSE).

Dallaway, E. (2016). #ISC2Congress: Cyber crime Victims Left Depressed and Traumatized. Infosecurity Magazine. Retrieved July 4 2018, from https://www.infosecurity-magazine.com/news/isc2congress-cyber crime-victims

Deakin University 1994, Fraud against Organisations in Victoria, Deakin University, Geelong.

DESE Datasets (2022)

D'Rosario, M., Australia's significant Computing Legacy: Helping to Connect the World. Australian Policy and History. November 2010.

Dupont, B., 2013. Cyber security futures: How can we regulate emergent risks?. Technology Innovation Management Review, 3(7).

Ernst and Young 2003, The Unmanaged Risk, Ernst and Young, London.

Galeotti, A., Golub, B. and Goyal, S., 2020. Targeting interventions in networks. Econometrica, 88(6), pp.2445-2471.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q. & Laplante, P. (2011). Dimensions of cyber attacks: Social, political, economic, and cultural. IEEE Technology & Society Magazine, 30(1), 28-38

Gretton, P., Gali, J. and Parham, D., 2004. The effects of ICTs and complementary innovations on Australian productivity growth. The Economic Impact of ICT: Measurement, evidence and implications, pp.105-30.

Gretton, P., Gali, J. and Parham, D., 2004. The effects of ICTs and complementary innovations on Australian productivity growth. The Economic Impact of ICT: Measurement, evidence and implications, pp.105-30.

(ISC)2® Datasets (2021)

Juneja, A., Juneja, S., Bali, V., Jain, V. and Upadhyay, H., 2021. Artificial intelligence and cyber security: current trends and future prospects. The Smart Cyber Ecosystem for Sustainable Development, pp.431-441.

Kirwan, G. & Power, A. (2011). The Psychology of Cyber Crime: Concepts and Principles. IGI Global.

Lemley, M.A. and Lessig, L., 2000. The end of end-to-end: Preserving the architecture of the Internet in the broadband era. Ucla L. Rev., 48, p.925.

Lessig, L. (1999). Code and Other Laws of Cyberspace. NY: Basic Books.

Lessig, L., 1995. The path of cyberlaw. The Yale Law Journal, 104(7), pp.1743-1755.

Lessig, L., 1995. The zones of cyberspace. Stan. L. Rev., 48, p.1403.

Mayhew, P. 2003, Counting the Costs of Crime in Australia: Technical Report, Technical and Background Paper Series, no. 4, Australian Institute of Criminology, Canberra, http://www.aic.gov.au/publications/tbp/tbp004.html.

Modic, D., & Anderson, R. (2015). It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud. IEEE Security & Privacy, 13(5), 99-103.

Naidoo, V. and Verma, R., 2020. Unpacking Cyber security Trends. In The Evolution of Business in the Cyber Age (pp. 321-338). Apple Academic Press.

NSC, National Skills Commission datasets (2022)

Nurse, J. R. C. & Bada, M. (2018). The Group Element of Cyber crime: Types, Dynamics, and Criminal Operations. In Attrill-Smith, A., Fullwood, C. Keep, M. & Kuss, D.J. (Eds.), Oxford Handbook of Cyberpsychology 2nd Edition. Oxford: OUP. https://doi.org/10.1093/oxfordhb/9780198812746.013.36

Nurse, J. R. C. (2018). Cyber crime and You: How Criminals Attack and the Human Factors that They Seek to Exploit. In Attrill-Smith, A., Fullwood, C. Keep, M. & Kuss, D.J. (Eds.), Oxford Handbook of Cyberpsychology 2nd Edition. Oxford: OUP. https://doi.org/10.1093/oxfordhb/9780198812746.013.35

Nurse, J. R. C., Creese, S., & De Roure, D. (2017). Security risk assessment in Internet of Things systems. IT Professional, 19(5), 20-26. IEEE. https://doi.org/10.1109/MITP.2017.368095

NCVER Datasets (2022)

CyberCX