NSW Cyber Business Exchange

Cyber Skills Study Report 2024

The NSW Cyber Business Exchange is a NSW Government Funded Program

AISA

Australian Information Security Association

Introduction

The NSW Cyber Business Exchange is an Investment NSW Government funded program, delivered in partnership with the Australian Information Security Association (AISA). An objective of the program was to shed light on the skills, competencies and roles available in today's Cyber Security Workforce, the gaps between what is available and what is in demand, and the skills and competencies that will be required for the roles that will be in demand in the next three years. The following report addresses the objective.

Acknowledgements

Research, analysis, and benchmarking against industry best practice both nationally and internationally was undertaken by researcher Dr Chris Culnane and Dr Suelette Dreyfus.

Dr Culnane is an Honorary Fellow at the University of Melbourne who specialises in privacy and web security, as well as being an independent security consultant at Castellate Consulting Ltd.

Dr Dreyfus is an AISA Board Member and Senior Lecturer at The School of Computing and Information Systems at the University of Melbourne, where she teaches digital privacy and information security.

Table of Contents

Executive Summary

There has been considerable public debate about the causes of the labour shortage in cyber security in Australia. Government has stepped in with a number of activities to improve this shortcoming. However, as well as being a problem of national importance, the shortage is also a complex problem to solve well. Solving thorny problems with long pipelines often requires several phases of responsive policy development and application. This includes taking mid-change measurements along the way to understand what is working, what is not, and how to address those sticky problems that persist.

To that end, AISA undertook a large-scale survey of the industry between January and March 2024 in order to understand where there are still skills gaps for entry level cyber security industry entrants and what is required to address any gaps. The survey design was informed by prior cyber security programs from Investment NSW[1], [2] and the wider NSW Government cyber strategy.[3] This report examines the results of that survey, in the context of other industry analysis.

Industry survey respondents were asked to rate both the importance of various cyber security competencies as well as how large they perceived the skills gaps to be for those competencies.

Whilst the majority of respondents view the competencies as being very important, there are differences in the rating based on the size and industry of the organisation. This demonstrates the need for a nuanced approach that does not assume a one-size-fits-all strategy will deliver solutions across different industries and organisations.

Skills gaps remain a concern, particularly in some specialist cyber security areas. Views on Artificial Intelligence (AI) varied, with it receiving the lowest overall rating in terms of importance, but simultaneously being viewed as having the biggest skills gap. Whether the perception of this skills gap is valid, or if it is being driven by hype and fear remains unclear. Qualitative responses indicate divergent views, with some viewing it as a saviour that will replace existing cyber security roles, whilst others viewed it as increasing the cyber risks as new tools and attack surfaces become commonplace.

Cyber security continues to grow and remains in-demand with shortages across core cyber security roles. Whilst there has been some softening in related roles, the expected demand for core cyber security roles remains projected to exceed the economy-wide average.

The field is suffering from over complication in both how it is described and in terms of the breadth of certifications available. This is not unique to Australia or NSW, but nonetheless is a challenge that needs to be faced. Among other improvements, greater clarity in how career pathways are designed, presented and communicated is needed particularly for new or reskilling entrants.

1 https://www.investment.nsw.gov.au/focus-sectors/technology/cyber-security/
2 https://www.investment.nsw.gov.au/focus-sectors/technology/cyber-security/cyber-industry-experiences/
3 https://www.digital.nsw.gov.au/delivery/cyber-security/strategies

Key Findings

- The majority of organisations of all sizes continue to maintain in-house cyber security capabilities.
- Respondents who were not responsible for hiring staff tended to rate competencies as more important than those who were responsible for hiring.
- All cyber competencies, with the exception of AI Security were rated as “Extremely important” or “Very important” by the majority of respondents.
- Different industries rated the importance of competencies differently.
- The size of the organisation (number of employees) impacted on how important respondents considered competencies. Smaller organisations tended to rank competencies as more important when compared to large organisations.
- The majority of respondents rated AI Security as only “Somewhat important” or “Less important”. All other competencies had a majority of respondents rating them as “Extremely important” or “Very important”.
- Contrasting with its importance rating, AI Security was rated as having an “Extremely large” or “Very large” gap by a greater proportion of respondents than any other competency.
- Industry had a lesser, but still discernible, impact on the perceived skills gap. Size and hiring responsibility did not have a discernible impact.
- Jobs and Skills Australia data indicates that the shortages for cyber security specific roles remain, and that demand is expected to continue to grow beyond the economic average.
- Cyber security leadership roles do not indicate a shortage. A few cyber related development roles are no longer in shortage, with many now projected to see growth consistent with the economy wide average in comparison to beyond economy wide growth in demand in previous years.

Recommendations

Recommendation 1:

Prospective employers and students should pivot toward relying on skills pathways rather than certification-based pathways.

Recommendation 2:

Organisations in Australia need to recognise that all new cyber security hires will need training inside their new position.

Recommendation 3:

There is a very real role for government at a state and national level to expand support for bringing industry and cyber security education providers closer together specifically to build better student outcomes.

Recommendation 4:

Students and future workers need better, clearer information about the skills and knowledge pathways, so they can make more informed choices.

1. Current state of the cyber security workforce

1.1 Background

A Cyber Security skills shortage has been identified for a number of years, across Australia as a whole[4] and New South Wales (NSW) specifically[5]. AISA's 2020 study showed 25% of executives reported being constrained by being unable to find talent. The 2024 survey aims to look further at the state of the workforce and again look at what skills gaps exist within the cyber security job market.

1.2 States

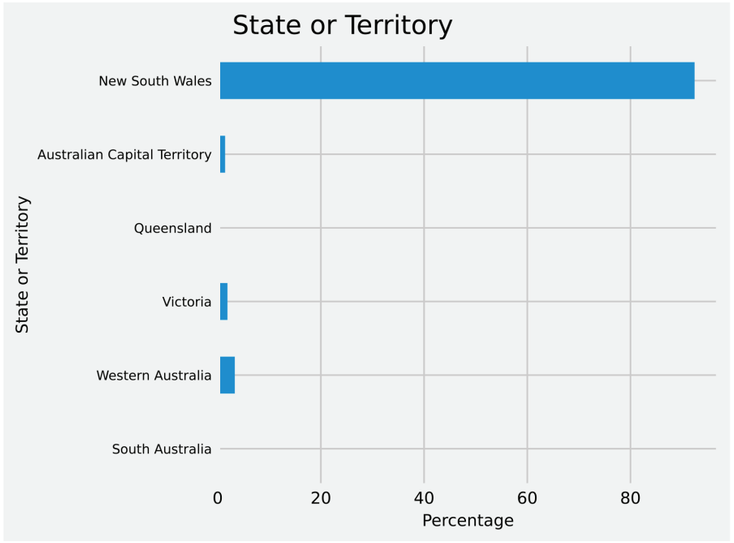

Figure 1. Plot of Responses by State

The survey, whilst targeted at NSW, was open to the whole of Australia. However, the number of responses from outside of NSW were low. Of the 211 valid responses that were received just 16 were received from outside of NSW, with only single responses from South Australia and Queensland, and no responses from Tasmania and the Northern Territory. As such, breaking down results by state would not be statistically significant as states other than NSW do not have sufficient sample sizes.

For structural analysis, the complete dataset has been presented. However, for competency analysis the results presented are for NSW only. This is due to analysis showing that there were indicators of statistically significant differences in responses for non-NSW participants to some competency questions. Specifically, for the question on the most important competencies the Secure Programming competency was statistically significantly different. Similarly, for the question on the biggest competency gaps both the AI Security and Secure Programming competencies indicated statistically significant differences.

4 https://www.austcyber.com/resources/sector-competitiveness-plan-2019/chapter3
5 https://www.aisa.org.au/Public/Public/AboutAISA/Research/skills-and-jobs-study.aspx

1.3 Structure and Provisions

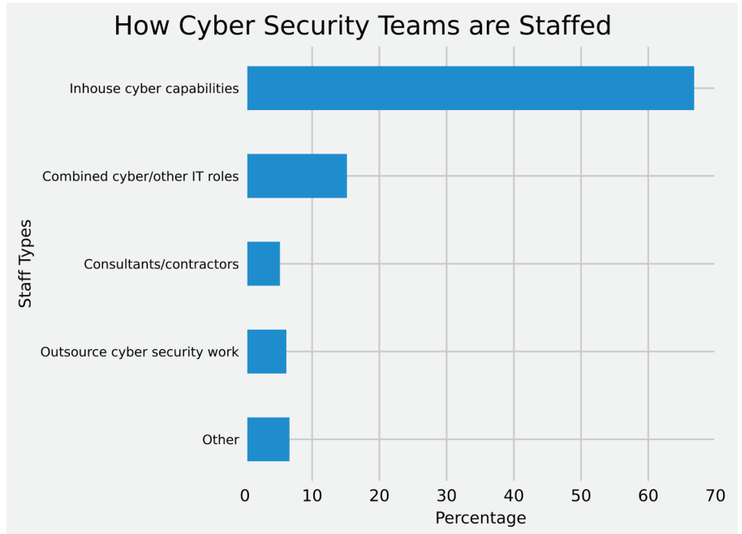

Figure 2. Plot of Staffing Methods

68.8% of respondents indicated that they staffed their cyber security teams via in-house appointments, with only 11.4% using either contractors or outsourcing, see Figure 2. Whilst there are differences between industries they are not statistically significant. Most of the respondents who selected 'Other' indicated that they used a combination of some or all of the methods for staffing their cyber security teams. This indicates organisations continue to maintain in-house cyber capabilities.

Figure 3 shows what organisations do in regards to cyber security. There are some indicators that respondents have interpreted this question potentially differently to what was intended. Specifically, that the majority of respondents indicated their organisations "Provide cyber security education, training or credentials". We can speculate that this is likely a result of respondents interpreting the provision of training to include in-house cyber security training, rather than as a broader training provider.

We can further break down the responses by industry, as shown in Figure 4. Education is joint highest (25%) with Energy/Utilities in terms of the percentage of respondents indicating they specifically provide cyber education, training or credentials. The sample size for Energy/Utilities is relatively small (4) but even industries with larger sample sizes, for example, Consulting (36) and IT Services (37) have a high percentage of respondents indicating they provide education, training or credentials, at 13.9% and 13.5% respectively.

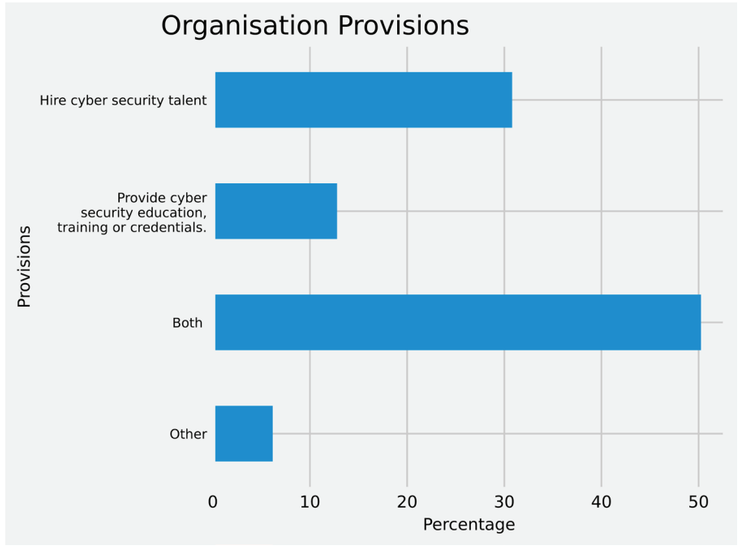

Figure 3: Plot of What Organisations Do

When looking at the combination of responses that were “Both” or “Provide cyber security education, training or credentials”, i.e. all organisations that provide some education, training or credentials, and that have a reasonable sample size (above 10), Education is not the leading industry at 70%, that is Managed Security Services at 72.2%. As such, we can conclude that it is likely the question has been interpreted by at least some respondents to include in-house training. As such, we will not use the responses from this question in any further cross-tabulation as we cannot reliably determine the interpretation of the responses.

Organisation size does not appear to have a strong influence on the staffing methods. In particular, the majority of small to medium organisations (less than 100 employees) maintain in-house cyber capabilities. Of interest is that the proportion maintaining such capabilities exceeds the equivalent proportion for organisations of 100-1000 employees. This may indicate that organisations face challenges when growing to maintain in-house capabilities. Consistent with this is that organisations with between 100 and 1000 employees have the highest proportion of outsourcing at 12% compared to 9% for organisations with less than 100 employees. Furthermore, the percentage of outsourcing declines as organisations grow, with 4% for organisations with 1001-5000 employees and 2% for organisations with over 5000 employees.

2. Role and competencies in demand

To evaluate the in-demand competencies respondents were asked “What are the most important cyber security competencies for someone entering a career in cyber security?” and asked to rate them as to importance for their organisation. For consistency, the list of competencies were taken from the United States of America’s National Institute of Standards and Technology (NIST) National Initiative for Cyber security Education (NICE) NIST NICE[6] framework

Figure 4: Plot of What Organisations Do By Industry

Due to small sample sizes and statistically significant differences in responses between respondents from NSW and those from elsewhere, for a number of competencies, the results below are for NSW only.

A high-level summary of the results, as shown in Figure 6, is as follows:

- With the exception of AI Security, the majority of respondents rated all the competencies as either “Extremely important” or “Very important”.
- The most important competency was Cyber Security Fundamentals, with over 94% rating it as “Extremely important” or “Very important”.
- The second most important competency was Data Security with over 91% rating it as “Extremel important” or “Very important”.
- AI Security was an outlier with only 39% of respondents rating it as “Extremely important” or “Very important”.
- With the exception of AI Security, no other competency received less than 60% of respondents rating it as “Extremely important” or “Very important”.
- Very few respondents rated any of the competencies as “Not Important”, with the highest percentage being 5% for Operational Technology (OT) Security[7].

6 https://www.nist.gov/itl/applied-cybersecurity/nice
7 Operational Technology Security: ”OT encompasses a broad range of programmable systems and devices that interact with the physical environment (or manage devices that interact with the physical environment).” - NIST https://csrc.nist.gov/pubs/sp/800/82/r3/final

As such, the results do not provide much of a priority list, in other words, everything, with the exception of AI Security, is “Very important” or greater.

Whilst an overarching priority list cannot be constructed, we can see that there are statistically significant differences in the responses between different industries, sizes of organisations, and even whether the respondent was responsible for hiring or not.

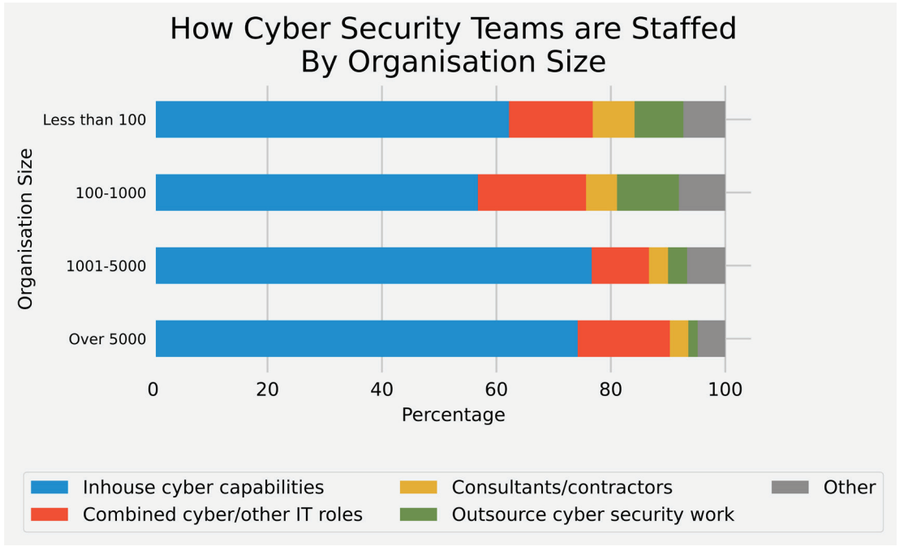

Figure 5: Plot of Staffing Methods by Organisation Size

2.1 Hiring Responsibilities

When evaluating the differences in responses between those who were responsible for hiring and those who were not, we can see statistically significant differences in some competencies, as shown in Figure 7a and Figure 7b respectively. The specific competencies where this was observed were:

- Communication Security
- Data Security
- OS Security (Operating System Security)
- OT Security (Operational Technology Security)

In all four cases those who were NOT responsible for hiring rated those four competencies as having more importance than the respondents who were responsible for hiring. Whilst this was only observed at statistically significant levels for the stated four competencies, the ratings were higher across all competencies, except Cyber Security Fundamentals, for those not responsible for hiring. This indicates that those performing the hiring within an organisation could be diverging from their colleagues.
The root cause of this cannot be determined from this survey, however, it raises an interesting future question for possible further exploration.

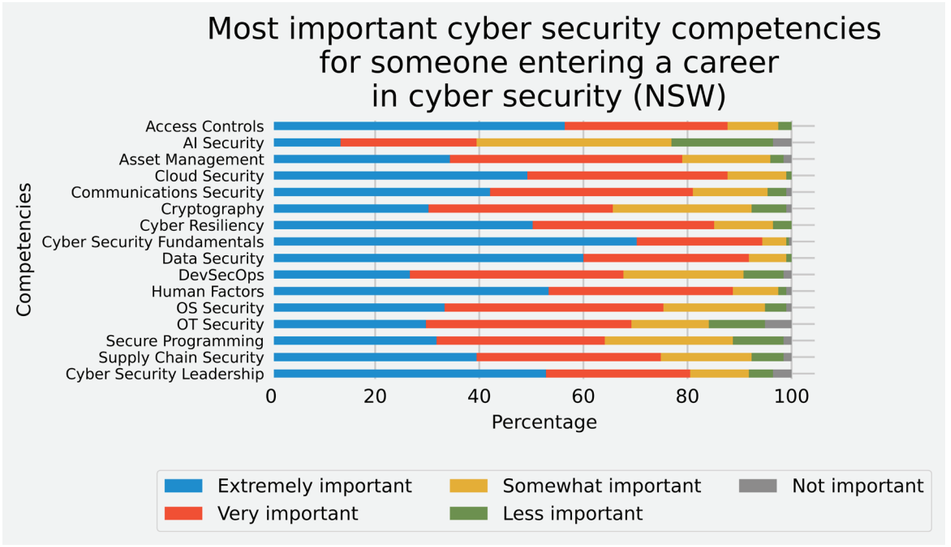

Figure 6: Plot of the importance of cyber security competencies for someone entering a career in cyber security

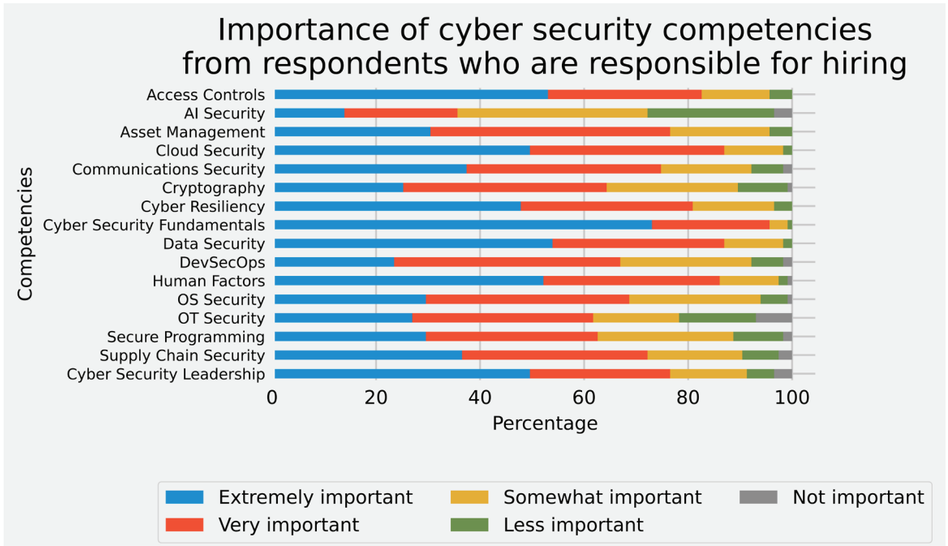

Figure 7: With and Without Hiring Responsibility: Impact on Importance Rating

a) Importance of competencies from respondents responsible for hiring

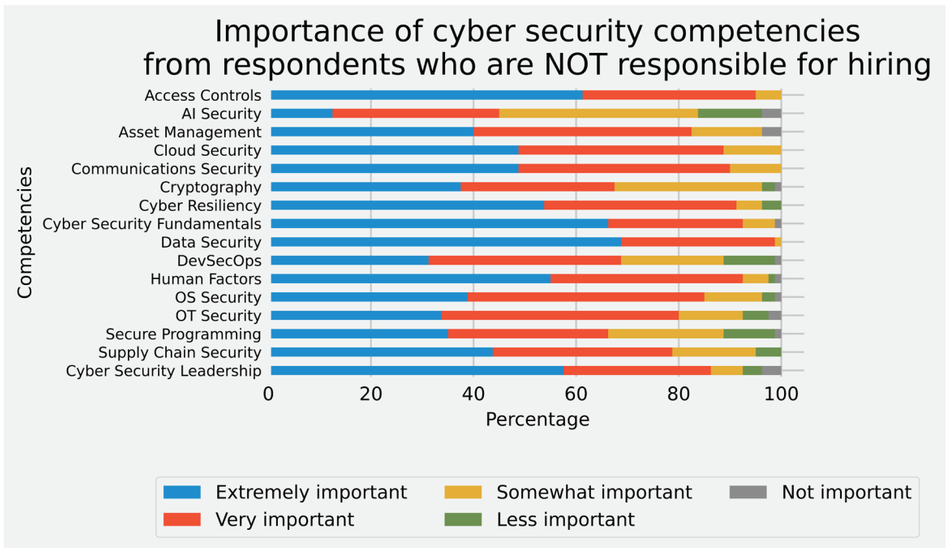

Figure 7: With and Without Hiring Responsibility: Impact on Importance Rating

(b) Importance of competencies from respondents NOT responsible for hiring

2.2 Industry

The data reveals that different industries rate competencies differently with a number of instances of statistically significant differences. The following are some examples to illustrate the observation for the industries with the most responses (Managed Security, IT Services, Consulting, Education, Government) and for competencies that have statistically significant differences.

2.2.1 Education

Education shows statistically significant differences for a number of competencies, but the most prevalent is for AI Security. Figure 8 shows just the AI Security competency broken down by the different industries. If we focus only on those with a reasonable sample size, shown in the brackets, we can see that there is a significant difference between Education and Managed Security, Consulting, and Government, with Education rating AI Security as more important, particularly in contrast to Government.

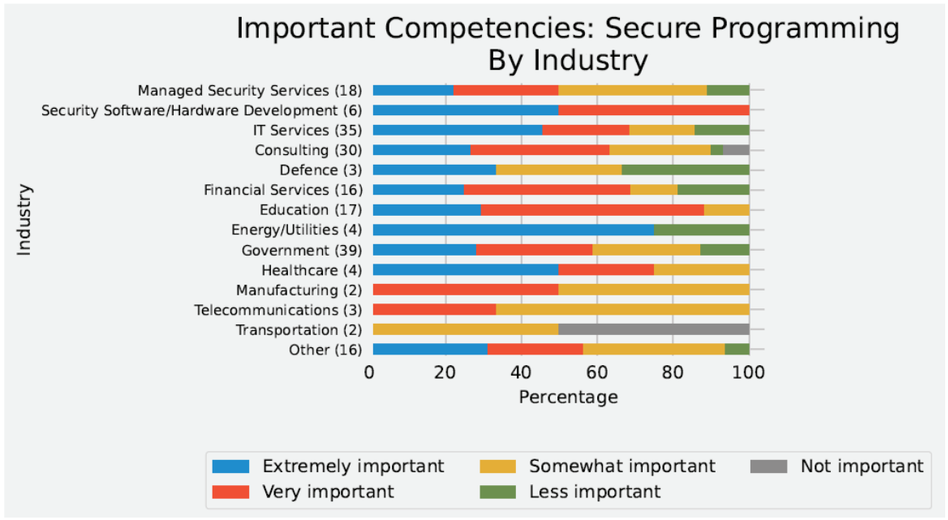

Figure 8: Plot of the importance of AI Security by Industry

Education and Consulting showed four instances of a significant difference. Those differences were seen for AI Security, Communication Security, Cryptography, and Data Security. Plots for Communication Security, Cryptography, and Data Security are included in Appendix B.4 in Figure 19, 20, and 21 respectively. In all four instances Education rated those competencies as of higher importance than Consulting. One possible explanation could be that those four competencies are more aligned with traditional education subject areas, which may cause a bias towards their importance. However, that is only conjecture, further research would be required to establish the definitive cause.

2.3 Consulting

As already discussed, Consulting and Education exhibited different attitudes to the importance of a number of competencies. Consulting also exhibited statistically significant differences in attitude to the importance of a number of competencies when compared to the attitudes from other industries. Those industries were Managed Security, IT Services and Government. The competencies where there was statistically significant differences in attitude are shown below for each of those industries:

- Managed Security
  - OS Security

- IT Services
  - Communication Security
  - Data Security
  - OS Security
  - OT Security

- Government
  - Communication Security

Further figures for OS Security and OT Security can be found in Appendix B.4 in Figure 22 and 23 respectively. In each of the instances, Consulting rated the competency as less important than other industries.

The overall conclusion that can be drawn is that different industries assess the importance of the competencies differently. This stands to reason, since different industries will face different threats, opportunities and working practices.

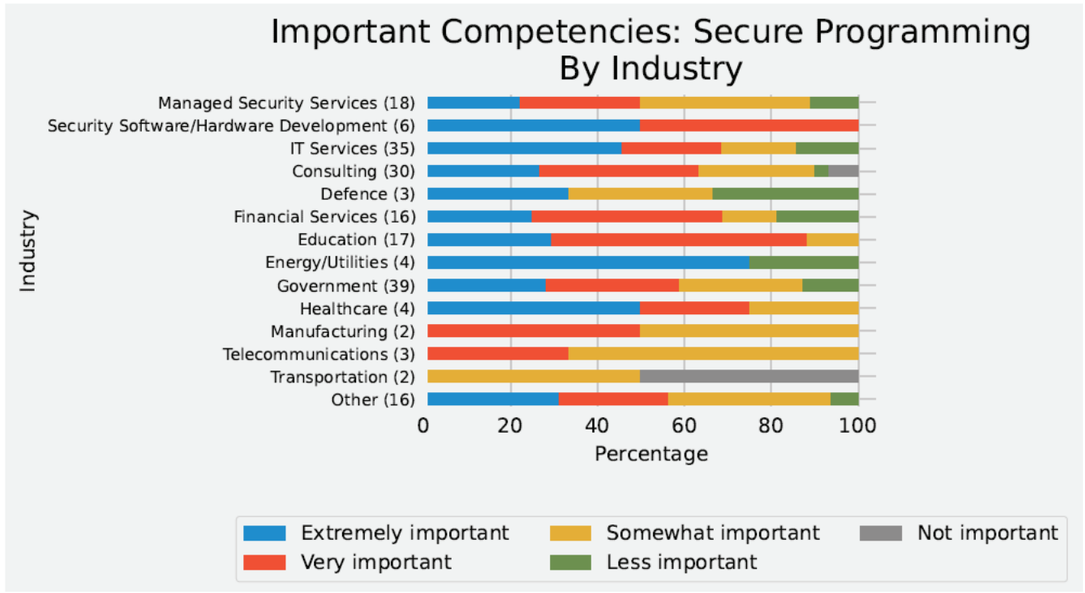

Figure 9. Plot of the Importance of Secure Programming by Industries in NSW

For example, in Figure 9, which shows the responses for Secure Programming, it is no surprise that all respondents in Security Software/Hardware Development rated it as "Extremely important" or "Very important", since that is a competency at the core of their business. Whereas Government rated it comparably lower, possibly because the Government is not undertaking large amounts of software development.

As such, any measures taken to target or address specific competencies should be cognisant of the industry sectors that such measures are intending to target.

2.4 Organisation Size

In addition to the already discussed differences, there is evidence that the size of the organisation also impacts on the perception of the importance of a number of competencies. In particular there are statistically significant differences between organisations with less than 100 employees (small) and organisations with more than 5000 employees (large). That in itself is not surprising, as the differences in organisational capability and scope are likely to impact on perceived needs.

However, what is somewhat surprising is that the smaller organisations consider a number of competencies as being more important than the larger organisation. Specifically, Asset Management, Cloud Security, Human Factors, OT Security, and Supply Chain competencies. In all cases, a greater proportion of respondents from smaller organisations rated those competencies as either "Extremely important" or "Very important". This is shown in Figure 10a for small organisations vs. Figure 10d for large organisations. This is particularly noticeable for the "Extremely important" rating. For example, 58% of small organisation respondents rated Cloud Security as "Extremely important", whilst only 41% of respondents from large organisations gave it the same rating.

This is surprising, as it is likely that large organisations face far greater exposure to cloud security given their greater use[8] - in terms of both breadth and depth - of such services, and therefore their increased attack surface. Similarly, OT Security is unlikely to be the preserve of small organisations, yet, 41% of respondents from small organisations rated it "Extremely important" compared with only 17% for large organisations.

In general, smaller organisations rated more competencies as more important in larger proportions. This could be as a result of a lack of understanding or the different competencies, and therefore the application or relevance to their own businesses. But even if that were the case, this presents the possibility that small organisations are incorrectly targeting their resources or looking for unrealistic job candidates who have a breadth of skills that is not practical or possibly not required.

Whilst the statistically significant differences were confined predominately to differences between large and small, there was also one significant difference between organisations with 100-1000 employees and large organisations. Organisations with 100-1000 employees rated the *Asset Management* competency more highly than large organisations, as shown in Figure 10b and Figure 10d respectively.

8 https://www.abs.gov.au/statistics/industry/technology-and-innovation/characteristics-australian-business/2019-20

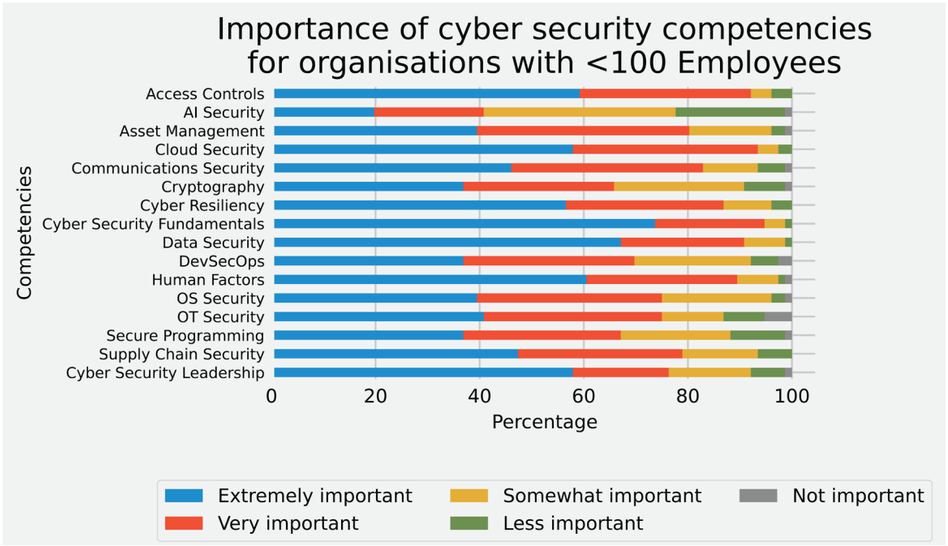

Figure 10: Size of organisation Impact on importance Rating

(a) Importance of competencies from organisations with <100 employees

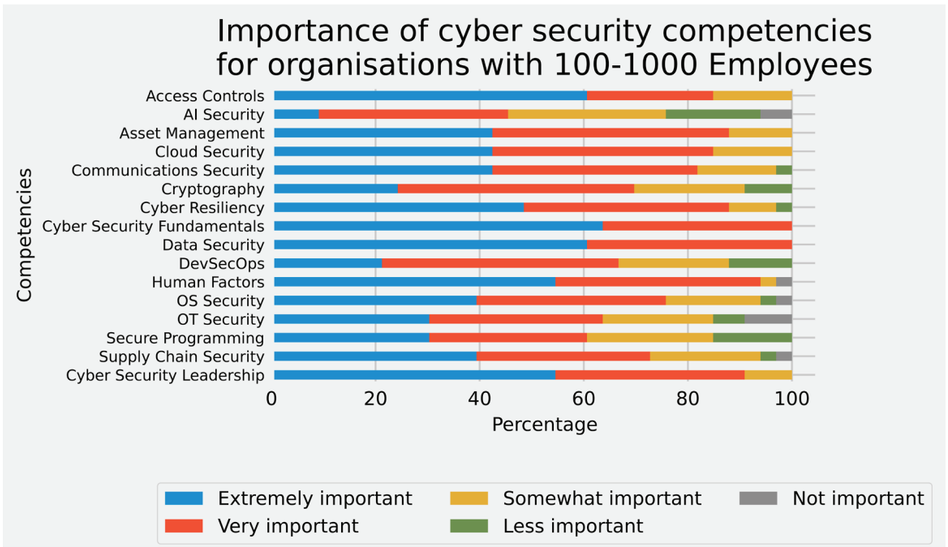

Figure 10: Size of organisation Impact on importance Rating

(b) Importance of competencies from organisations with 100-1000 employees

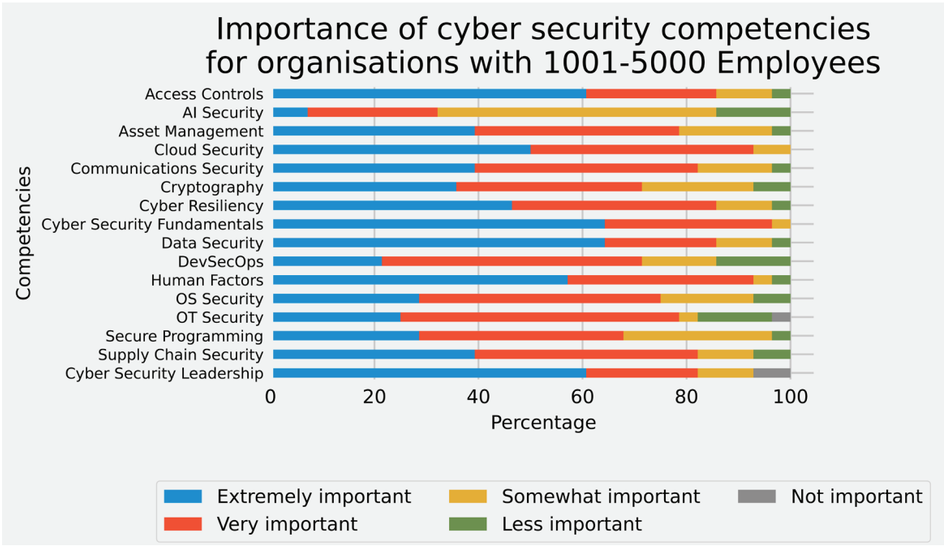

Figure 10: Size of organisation Impact on importance Rating

c) Importance of competencies from organisations with 1001-5000 employees

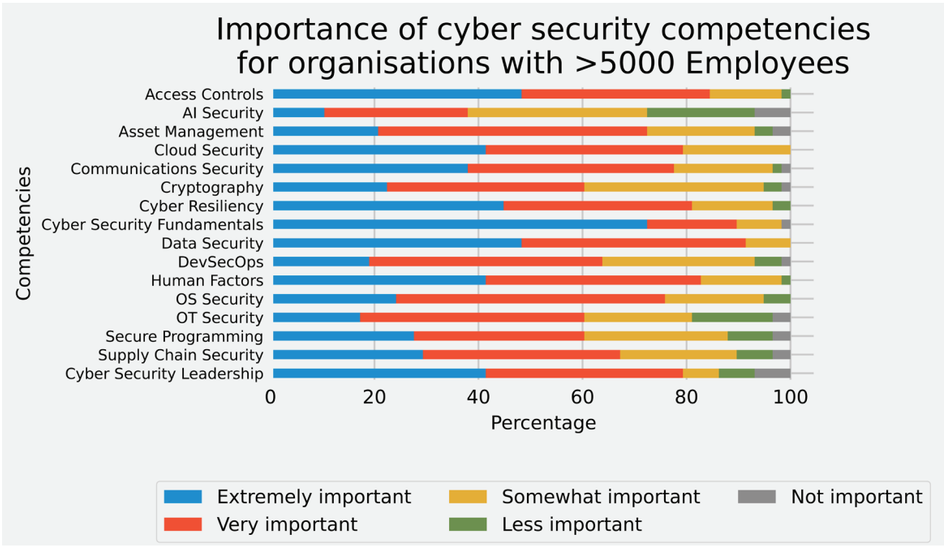

Figure 10: Size of organisation Impact on importance Rating

(d) Importance of competencies from organisations with >5000 employees

2.5 Qualitative Responses

In addition to providing ratings of importance, respondents were also asked what competencies were missing from the list shown. 70% of respondents left some form of text comment. Common themes suggested were as follows (the code word(s) and percentage of responses containing them are shown in brackets):

- People or soft skills (People 6.7%, Soft 3.6%)
- Communication both internal and external (Communication 8.2%)
- Risk Management (Risk 8.7%)
- Incident response (Incident 5.1%)
- Networking (Network 4.1%)
- Compliance (Compliance 4.6%)
- Continued Learning (Learn 6.7%)

Whilst the question asked for competencies, many of the respondents provided a list of skills they perceived as missing from the list. Furthermore, the skills that were listed, with the possible exception of Continued Learning, are already covered by various competencies within the NIST NICE framework.

As such, these responses indicate that respondents may not have understood the question, and may have been indicating a ranking or preference for skills already encompassed by the listed competencies instead of addressing perceived deficiencies.

An alternative explanation could be that some of the respondents have limited exposure or understanding of NIST NICE competency areas. Whilst the NIST NICE framework is comprehensive, there is a lot of detail to be consumed, and the framework has recently undergone its first major revision that has caused some terminology to change[9]. If a lack of familiarity is the cause, it would be hoped that over time this would improve as more people consume and become accustomed to the framework.

However, some assistance may be needed for small organisations who may not have the capacity to ingest the entire framework and may require some signposting and guidance about where to look and what priorty areas should be consumed first. Whilst there are some tools available[10], they have only recently (June 2024) been updated to reflect the revisions to the framework and are US centric and assume a degree of understanding of the framework to be able to be used effectively.

2.6 AUCyberExplorer Data

Futher data on demand and supply of cyber security jobs is available via AUCyberExplorer[11]. For the period from the 1st February 2022 to 31st January 2023, it indicates there were 4,858 cyber related job openings in NSW (2,592 were dedicated cyber roles, whilst 2,266 were cyber related). 88% of those were based in Sydney. The bulk of those jobs were in two NIST NICE categories; *Securely Provision* and *Operate & Maintain*[12]. The supply/demand ratio, indicating the number of qualified workers to the job openings, is 9.31 for NSW, slightly lower than the national average of 9.56 and Victoria's 10.03. The bulk of the jobs (1,038) were in the financial services industry.

By comparison, AUCyberExplorer indicates that Victoria had 3,544 cyber related job openings, of which 1,734 were dedicated and 1,810 were cyber related. 91% of the job openings were based in Melbourne. Again the bulk of the jobs fall in the *Securely Provision* and the *Operate & Maintain* (now Implement and Operation) NIST NICE categories. However, there is a slightly higher proportion of jobs in Oversee & Govern (now Oversight and Governance) and the Protect & Defend (now Protection and Defense) categories, although the difference is marginal. The bulk of the jobs were in the Healthcare and Social Assistance industry.

Across Australia as whole, NSW and Victoria dominate the cyber security job market, with Queensland 3rd with 1,725 cyber job openings. This is followed by Australian Capital Territory (1,561), Western Australia (769), South Australia (523), Northern Territory (91), and Tasmania (89).

2.6.1 Certification

AUCyberExplorer also provides data on certification numbers compared with job openings requesting such certifications. Australia-wide there were 3,260 CISSP (Certified Information Systems Security Professional) holders and 1,066 openings requesting CISSP certification, giving a ratio of 3.1 to 1. Conversely, there were 1,929 CompTIA (Computer Technology Industry Association) Security+ holders, but only 122 openings requesting it, giving a ratio of 15.8 to 1. The ratio for the Global Information Assurance Certification (GIAC), for which there were 3,587 holders compared with only 124 openings requesting it, was 28.9 to 1. We cannot definitively say why there are such differences in ratios, but one possibility is that CompTIA Security+ and GIAC are being used as part of Continuing Professional Development (CPD), which would cause a growing number of holders even if employers are not specifically requesting such certifications in their job advertisements.

The CISSP ratio is relatively stable across NSW (3.2) and Victoria (3.8). However, there is a big difference for CompTIA Security+ ratio, which in Victoria is 32.4 compared with NSW's 12.6. This difference is primarily due to there being far fewer jobs requesting CompTIA Security+ in Victoria. This could be due to the significantly different industry make up between NSW and Victoria. Further analysis of the data indicates the number of holders is broadly similar, with 667 holders in NSW and 551 in Victoria. The difference in ratio is due to the differences in the number of jobs requesting it, with 53 in NSW and 17 in Victoria. Both are low numbers, but it would appear that businesses in Victoria ask for it less, despite having a proportionally similar number of holders available in the job market.

Most of the cyber security jobs are in the categories related to design, development and implementation. Specialist categories like Intelligence and Cyber Effect are significantly fewer in number.

In summary the AUCyberExplorer reveals that different certifications hold different value in different states. It also reveals some certifications appear to have little demand within the job market despite fairly widespread adoption. This highlights the challenges faced by those entering the cyber security job market in determining what certification is most appropriate and valuable.

9 https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-history-and-change-logs
10 https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool
11 https://www.aucyberexplorer.com.au/maps/current-supply-demand

12 The Securely Provision and Operate & Maintain NIST NICE categories have since been renamed in the framework to Design and Development and Implementation and Operation respectively.

3. The workforce skills gap

Respondents were asked to rate what they thought were the biggest competency gaps, rating each of the NIST NICE competency areas between “Extremely large gap” and “Not gap”.[13]

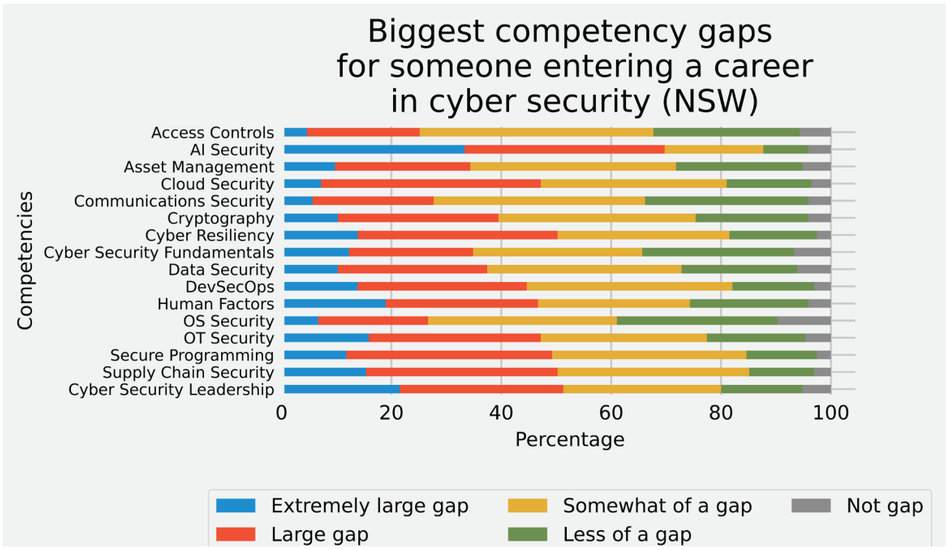

Figure 11. Plot of the biggest competency gaps for someone entering a career in cyber security in NSW

Figure 11 shows an overview of the responses for NSW. It is clear that for most of the competencies the majority of respondents considered there to be either “Somewhat of a gap” or less. Those competencies where that was not the case were AI Security (70%), Cyber Resiliency (50%), Supply Chain Security (50%), and Cyber Security Leadership (51%), which had a 50% or higher proportion of responses indicating a “Large” or “Extremely large” gap.

Of note is that the AI Security competency is deemed by the most people to have the largest gap when looking at either just “Extremely large gap” or the combination of “Extremely large” and “Large” gap. This is of interest since this was also the competency which was deemed as having the least importance. It would be desirable for a highly ranked competency, in terms of importance, to have a low gap rating. This would be the ideal scenario since it would indicate the closing of the skills gap. There is evidence of such competencies, for example Access Control, which was ranked by 88% of respondents as “Extremely” or “Very” important, and has the lowest rated gap, with only 25% of respondents indicating an “Extremely” or “Very” large gap. It is a similar case for Cyber Security Fundamentals, which 94% of respondents rate as “Extremely” or “Very” important, and had only 35% of respondents indicating an “Extremely” or “Very” large gap.

To explore whether there is a relationship between the perception of importance and gaps a correlation matrix was constructed, shown in Figure 11. A strong correlation would be shown as values closer to 1, with no correlation being values closer to 0. As can be seen there is no meaningful correlation between the responses to the two questions. In other words, the rating a person gave to the importance of a competency was not a good predictor of the rating they gave that same competency, or indeed any other competency, in terms of perceived gap.

13 The survey used the term “Not gap“ so for consistency we have used that in the report, we assume it was intended to represent “No gap”.

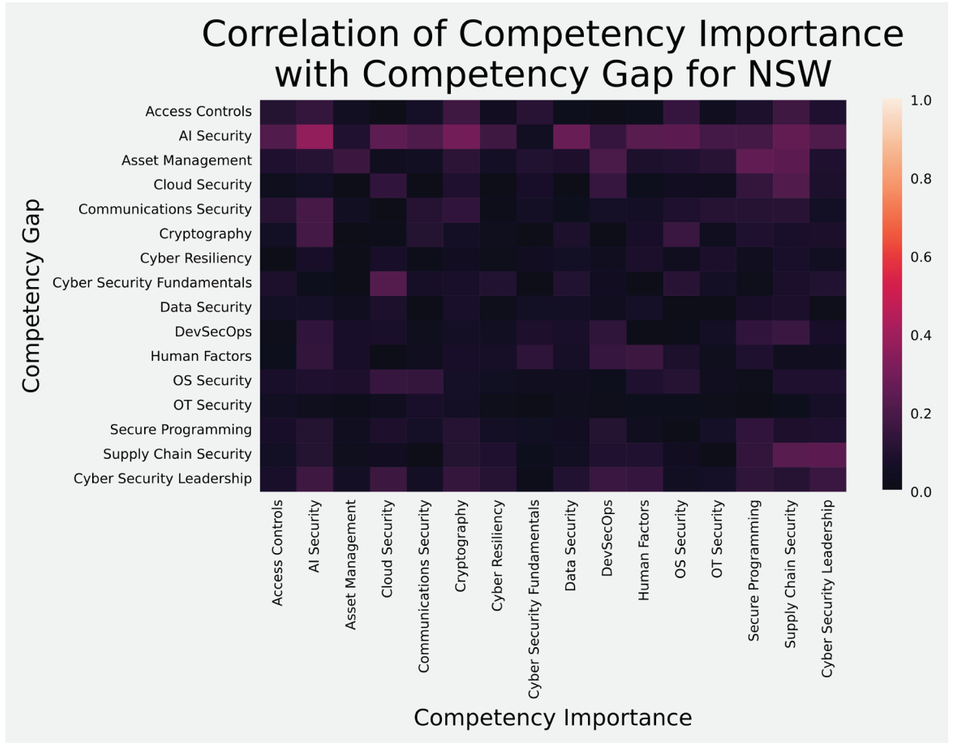

Figure 12: Plot of the Correlation between Importance and Gap of the Competencies in NSW

The lack of correlation indicates that the responses were largely independent between the two questions and therefore we cannot conclude that those who rated the competency as highly important were the same who perceived it to have a smaller gap. Similarly, we cannot conclude that those who perceived a competency as less important, and therefore may not have had first hand experience in hiring in such areas, are perceiving the gap to be smaller.

3.1 Hiring Responsibility and Size

Unlike with the evaluation of competency importance there was no statistically significant difference in responses between those who are or are not responsible for hiring. Nor was there a statistically significant difference between responses from individuals from different sized organisations. Plots showing a breakdown of the perceived competency gaps by organisation size are shown in Appendix B.4, in Figures 25a through 25d.

3.2 Industry

Similarly to the evaluation of the importance of different competencies, when breaking down the responses for perceived competency gaps we observe a statistically significant difference between industries for certain competencies. Again, we will focus on those industries that have a reasonable sample size (Managed Security, IT Services, Consulting, Education, Government).

3.2.1 Education

Education exhibited two statistically significant differences with Government for the OS Security and Cyber Security Leadership competencies. Plots for these two competencies are provided in Appendix B.4 in Figure 27 and Figure 28 respectively. In both cases respondents from Government perceived the gap as smaller than Education.

3.2.2 Consulting

Consulting exhibited a statistically significant difference with Managed Security for the competency of AI Security, as shown in Figure 26 in Appendix B.4. With Consulting having a much smaller proportion of respondents rating the gap as "Extremely Large" than for Managed Security.

3.2.3 Government

As already discussed, there were differences between Education and Government. Additionally, Government exhibited differences with Managed Security for AI Security, Cyber Resiliency and Cyber Security Leadership. In all cases, Government rated the gap as smaller than Managed Security did.

Overall, there were fewer differences in the perception of competency gaps than in the evaluation of the importance of competencies. This would indicate that there is a more consistent and uniform view on the perceived gaps.

3.3 Artificial Intelligence (AI)

As already discussed, there is a widespread perception of a "Large" or "Extremely large" skills gap in AI Security. This is somewhat surprising given the comparatively low level of importance AI Security was given in terms of importance. One possible explanation for this could be the perceived future growth, in that it is not currently an essential skill but could be in the future and therefore the perceived gap becomes more important. This is evidenced by the qualitative responses to the question that asked "What do you foresee to be the likely growth in cyber security personnel in your organisation over the next three years?" There were 142 responses to the question that were not N/A or blank. Of those 142 responses 17% mentioned AI, overwhelmingly the most common topic. For example, only 10% mentioned compliance, 9% mentioned Cloud, 8% mentioned risk, and only 2 people mentioned IoT (Internet of Things).

Whilst a number of respondents recognised the risks associated with the introduction of AI there were also some responses that indicated they viewed AI as the solution to cyber security skills gaps, since such jobs could transition to being done by AI.

Whether the AI Security skills gap is as large as perceived remains unclear. If we look at the responses to the question "Which of the in-demand roles have you had difficulty trying to fill in the last 12 months?" there were only 88 non-empty or non-N/A responses. Of those 88 just 3 mentioned AI. Conversely 10 mentioned Operational or OT roles, similarly Architecture roles were mentioned 10 times, and technical roles were mentioned 5 times. As such, it appears that real-world experiences of the skills gaps are in areas other than AI or AI Security.

3.3.1 AI Hype and Fear

The divergence between perception and reality may in part be caused by what has been significant hype, particularly over the last 18 months to 2 years, about the impending impact of AI. There has also been a propensity to create a Fear Of Missing Out (FOMO), with headline grabbing reports suggesting Australia is being left behind. For example, the Australian Computer Society's (ACS) report, Australia's Digital Pulse 2023, stated "One recent survey found Australian businesses currently lag in AI deployment, ranking 13th of 14 leading economies in 2022"[14]. That ranking is based on IBM's Global AI Adoption Index 2022[15]. What that statement did not mention is that Australia was only 1% behind the US and only 2% behind the UK. If Australia sees just an 8% increase in deployment it would move from 13th to 7th. The ACS report also revealed that students are twice as likely to have used Generative AI tools than employees. This was heralded as an advantage with the statement "When these students graduate and enter the workforce, they will transform how employees engage with and harness Generative AI."[16] This overlooks the significant cyber security risks such usage will bring.

Far from being a solution, AI could create new problems or re-introduce old ones. For example, a study in 2023 found that when ChatGPT was asked to generate 21 programs, in various different languages and with different purposes, only 5 of the 21 programs were initially secure. A further 7 were made secure after further interaction and refinement[17]. This is not an isolated finding, a different study on whether developers with access to an AI assistant write more insecure code found that "…participants who had access to an AI assistant wrote significantly less secure code than those without access to an assistant."[18]

Whilst we can expect further developments in AI, the likelihood that the promised capabilities will be realised in the near-term is increasingly under scrutiny. Even leaders in the field like Sam Altman, CEO of OpenAI, was quoted as saying "It's wildly overhyped in the short term,"[19] although he is confident in the long-term benefits.

The perceived AI Security gap raises a number of questions. Is it that there is a genuine gap? Is it just that AI has received so much coverage that it is dominant in respondents' minds even though they may not have sought to hire in AI Security? The qualitative responses indicate both hope and fear associated with AI and cyber security. However, the results do not necessarily support seeking to specifically address an AI Security skills gap. However, further research into how widespread AI usage is within cyber security, what protections are being deployed, as well as clear advice on the risks and benefits is likely to be beneficial to all organisations.

14 ACS Australia's Digital Pulse 2023, p.12
15 https://www.ibm.com/watson/resources/ai-adoption

16 ACS Australia's Digital Pulse 2023, p. 14
17 Khoury, R., Avila, A. R., Brunelle, J., & Camara, B. M. (2023, October). How secure is code generated by chatgpt?. In 2023 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 2445-2451). IEEE.
18 Perry, N., Srivastava, M., Kumar, D., & Boneh, D. (2023, November). Do users write more insecure code with AI assistants?. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (pp. 2785-2799).
19 https://fortune.com/2023/06/08/openai-ceo-sam-altman-a-i-wildly-overhyped/

3.4 Skills Shortage

Table 1 shows a mapping to the NIST NICE framework for the relevant cyber jobs from the Australian Jobs and Skill Priority List[20] along with their respective shortages and projected demand. The shortage and projected national future demand varies between roles. Cyber Leadership roles such Chief Information Officer (CIO) or Project Manager show no shortage and a projected growth at the economic average. This appears to be in contrast to the survey results, Figure 11, where Cyber Security Leadership was rated by the majority of respondents as having an "Extremely large" or "Large" gap. Whilst this appears to be a discrepancy with the survey results, it probably is not. The survey asked for skills gaps for someone entering a career in cyber security, whereas the skills shortage data is for the industry as a whole. As such, leadership skills would not be expected in a new entrant to a cyber security career. This may also help to explain some of the responses around AI Security, in that respondents may have been expressing their experience of what skills a new entrant had, not necessarily what skills they needed.

20 https://www.jobsandskills.gov.au/data/skills-shortages-analysis/skills-priority-list

Most Design & Development roles indicate shortages, with the exception of ICT Business Analyst and Software and Applications Programmers. Support roles, such as ICT Support and Test Engineers are not marked as having a shortage and are expected to have a future demand consistent with the economy-wide average. Specialist Cyber roles across multiple NIST NICE categories, such as Cyber Security Analyst, Cyber Security Architect, and Cyber Security Operations Coordinator are shown as having both a shortage and expected above economy-wide average future demand.

Broadly speaking, roles that are dedicated Cyber Security roles, with the exception of some leadership roles, are facing a shortage, with future demand projected to be above the economy-wide average. Those development roles that have elements of cyber security, for example, Web Developer, are not expected to have above average future demand, but are still currently indicating a shortage. However, if we look back at changes between 2022 and 2023, many of those jobs were projected as having an above average future demand. Furthermore, jobs like ICT Business Analyst have shifted from shortage to no shortage (across most states and territories).

When looking at the trend from 2022 to 2023 it appears as though the shortages associated with non-core cyber roles are starting to soften, both in current demand and future projected demand. However, core cyber security roles remain facing shortages.

ANZSCO	Category	Role	Occupation	National future Demand	National	NSW	VIC	QLD	SA	WA	TAS	NT	ACT
135111	OG	Executive Cybersecurity Leadership	Chief Information Officer										
135112	OG	Secure Project Management	ICT Project Manager										
135199	OG	Program Management	ICT Managers nec										
261111	DD	Enterprise Architecture	ICT Business Analyst										
261112	IO	Systems Security Analysis	Systems Analyst										
261211	DD	*No Mapping*	Multimedia Specialist										
261212	DD	Secure Software Development	Web Developer										
261311	DD	Secure Systems Development	Analyst Programmer										
261312	DD	Secure Software Development	Developer Programmer										
261313	DD	Secure Software Development	Software Engineer										
261314	DD	Systems Testing and Evaluation	Software Tester										
261315	DD	Secure Systems Development	Cyber Security Engineer										
261316	DD	*No Mapping*	Devops Engineer										
261317	PD	Vulnerability Analysis	Penetration Tester										
261399	DD	Secure Software Development	Software and Applications Programmers nec										
262113	IO	Systems Administration	Systems Administrator										
262114	OG	Cybersecurity Legal Advice/Privacy Compliance/Cybersecurity Policy and Planning	Cyber Governance Risk and Compliance Specialist										
262115	DD/OG	Software Security Assessment/Cybersecurity Architecture/Security Control Assessment	Cyber Security Advice and Assessment Specialist										
262116	PD	Vulnerability Analysis	Cyber Security Analyst										
262117	DD	Cybersecurity Architecture	Cyber Security Architect										
262118	CE	Cyberspace Operations	Cyber Security Operations Coordinator										
263111	PD/	Infrastructure Support	Computer Network and Systems Engineer										
263112	IO	Network Operations	Network Administrator										
263113	IO	Network Operations	Network Analyst										
263211	IO/DD	Systems Security Analysis/Systems Testing and Evaluation	ICT Quality Assurance Engineer										
263212	IO	Technical Support	ICT Support Engineer										
263213	DD	Systems Testing and Evaluation	ICT Systems Test Engineer										
263299	DD	Systems Testing and Evaluation	ICT Support and Test Engineers nec										

No Shortage	Shortage
At economy-wide average	Above economy-wide average

Table 1: Table shows the cyber relevant jobs and skill priority list

4. Preparing for the future

The NSW and Commonwealth Governments have already launched a series of policies likely to have a positive effect on the cyber security skills shortage. Examples of this include fee-free or fee-reduced TAFE qualifications in Cyber Security or related areas. This includes the option of a Cyber Security Traineeship, equivalent to between 655 and 970 hours, as part of a Certificate IV in Cyber Security. The standard course fee for both is $9,600, but depending on students' situations, up to the entire fee may be waived. However, there is more work to do in preparing for the future to match the demand in particular areas of cyber security.

The research findings in this report, based on the survey results and additional industry documents, point to a number of conclusions about the landscape of the future – and the need to address some challenges.

4.1 Awareness

There is now significant awareness about the importance of cyber security, the need to ensure that organisations have capacity in this area and a desire to both 'get into compliance' and to employ skilled workers in this space.

Perhaps only a handful of years ago, a medium sized business might have no staff with cyber security knowledge or qualifications. Now we see that the majority of even small to medium-sized businesses not only maintain cyber security capabilities, but they do so in-house. This suggests that both today, and looking forward, these business may want tighter control over their cyber security operations exactly because they understand how important it is to their organisation.

4.2 Continued growth in needed skills and knowledge

Online adversaries adjust their attacks with speed and often considerable resources. It's not possible for those working in cyber security to stand still; there is a long and ever growing list of technologies and concepts that a cyber security expert needs to be across. As a result, it can be difficult for employers to not only find the skills they are looking for in one candidate, but also even to identify what all those skills are. It is worth noting that government efforts to improve the labour shortage situation in this field have faced the added challenge of addressing a moving target over the past few years.

However, there is confusion among organisations about what specific skills they will need in new job hires in cyber security, and how hiring managers will measure these skills in applicants. This mirrors the confusion students experience as they try to answer the question 'But what certifications do I need to get a job in this industry?' Some of the confusion experienced by employers may be caused by the sheer volume of skills needed across all the different types of cyber security roles; some of it is also that new needs can arise rapidly, because of new threats.

NIST's NICE provides one framework for helping with this. Although its expansive size would make it difficult for an SME to cover all listed areas, the framework can help employers dimension a solution for specialty areas of need for example. Using it as a guide, SMEs can shape and trim NIST's NICE to their specific needs.

Meanwhile, students' confusion about what to study needs to be addressed at its source. Organisations must clearly define their requirements for students and education providers to ensure their needs are met. The planned development of a national framework with different pathways may provide some clarity. However, it is important that such pathways remain flexible and not rigid 'tick-box' exercises for micro-certifications ('micro certs'). Cyber security requires a mindset as much as any specific skill, and that is developed over time often through apprenticeships or work experience.

It is not surprising this problem exists; technology is moving quickly. Just staying abreast of one's own area of technical expertise at work may leave little room to also understand how artificial intelligence, machine learning and quantum computing may affect cyber security. Vendors use buzzwords that are running hot in the media to promote their latest software products. Hiring managers may believe these types of advances in technology will have more impact – and faster impact – than is actually the case.

A case in point is AI. A respondent to the survey said they intended to hire only law, communications or business qualified applicants because they expected that IT skills would be replaced with AI, off-shored or otherwise no longer needed.

The idea someone responsible for hiring would not hire someone with technical skills as they think AI will simply make that person obsolete in a very short time frame is concerning.

The reality is that machine learning, a subfield of AI, is improving the effectiveness of some cyber security software, for example by discovering and reporting anomalies in a more automated fashion, and at scale. However, that automation can only progress so far with existing technology. Machine learning, and AI more generally, are unlikely to replace a company's human cyber security unit in the near future. Humans are needed for great many things, including making sense of the information generated by these technologies. As for quantum computing, also mentioned by a respondent, it is likely to blossom into a genuine threat to cyber security (more particularly cryptography) some years into the future not immediately.

Finally, the survey participant's response about offshoring shows that going forward there is also a need to educate some industry decision-makers about the importance of data sovereignty. There are some legal requirements for this, but increasingly it is also an issue in the public discourse as Australians worry about their private information circulating outside the country in ways that may expose them to fraud or scam risks.

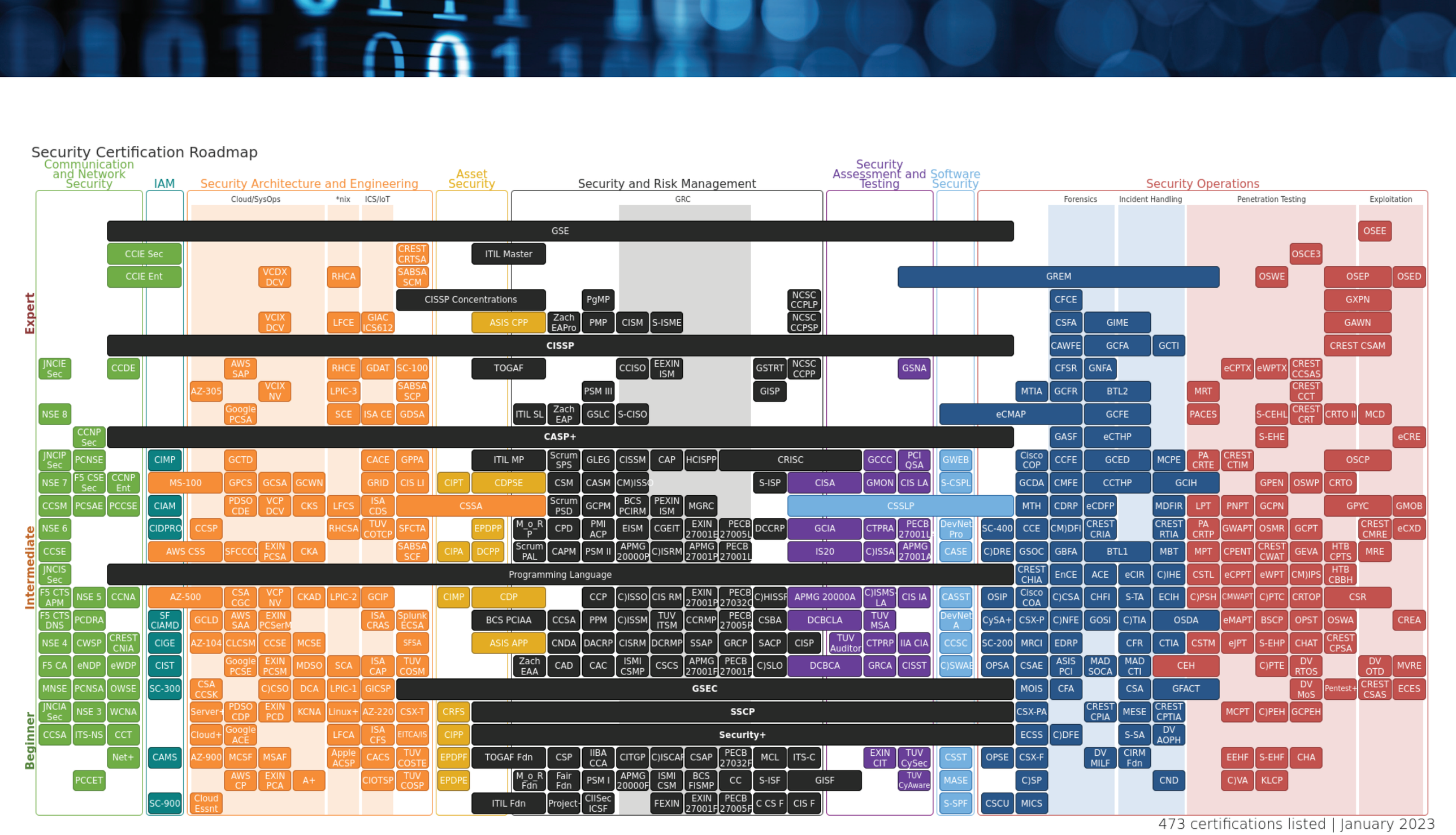

Figure 13: Security Certification Roadmap[21] By Paul Jerimy - All Credits to Paul Jerimy

21 https://pauljerimy.com/security-certification-roadmap/

This Security Certification Roadmap by Paul Jerimy, Figure 13 illustrates the very large number and variety of jobs in cyber security, from Security Architect to Risk Management and Governance, to Penetration Tester. No one could be qualified in all these areas at once. The Jerimy mapping sets out certifications available in each level in each area; it is a sea of micro certifications. It is not clear each micro cert provides the majority of the skills needed for that job. Further, skills required (eg, coding in Python) could very easily change with new products/technology, thus requiring an updating of skills and making 'the last micro certification achieved' not very valuable for getting a job or keeping it. It is far better for employers to focus on knowledge, experience and the specific skills they will need for the cyber security work in their business. From that point, they can present possible skills pathways they would like applicants to have followed. NIST's NICE framework work roles can assist employers as a guide in building a description of what they need.

The comprehensive nature of NIST's NICE framework provides a useful first stage model for growing the business community's awareness of the need to 'build in' cyber security across an organisation's diverse activities. However, as our later-stage analysis digs deeper into remaining problem areas, the necessity to also consider other frameworks becomes clear due to the size and detail of the NIST NICE framework.

Other models that may also be helpful to SMEs include those provided by UK Cyber Security Council[22] and CyBOK (The Cyber Security Body Of Knowledge)[23],[24]

Whilst the UK Cyber Security Council's Cyber Career Framework has benefits, the broader focus on a limited number of accredited degrees and the focus on advancing "professionalisation" of cyber security industry comes with risks. The obvious gate keeping risk needs to be addressed, particularly in an industry that already lacks diversity[25] and can ill afford to further hinder new entrants or lose existing members of its community. With the Federal government looking to support professionalisation through Shield 5 of the 2023–2030 Australian Cyber Security Strategy[26], caution should be adopted to ensure it creates an uplift and not a hindrance.

A strong focus on knowledge and skills above certification, with a range of traditional and non traditional pathways for demonstrating such skills is advised.

As Australia moves more toward defined pathways with 'professionalisation' categories, three things are of particular importance. First, proper recognition must be given to knowledge and experience when assessing competencies. While micro certifications can provide narrow skills of the day, they do not provide all that is needed for most cyber security positions. Chief Information Security Officers (CISO) in larger organisations may view that the 'right' person, once hired, can be enhanced with specific training modules such as a certification, but it does not follow that having a specific certification provides the 'right' person to hire.

Second, implementation of a 'professionalisation' scheme does not serve employers or staff well if the entity designing and updating the pathways also provides the qualifications. A complete separation of the two is necessary to ensure integrity in the pathway designs.

Third and finally, would-be cyber security workers should have a wide choice of providers, including TAFEs, universities, apprenticeships and micro cert companies, to 'complete' a given pathway.

22 https://www.ukcybersecuritycouncil.org.uk/
23 https://www.cybok.org/
24 https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework
25 https://www.rmit.edu.au/news/all-news/2023/apr/cyber-gender-report
26 https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

This will serve Australia best, since diversity of experience and knowledge is an advantage in this field and employers have enormously variable needs.

As such, to prepare for the future, Australia should pivot to skills and knowledge pathways. Flexible pathways should answer the student's question of 'How do I move into security testing?' with an outline of skills and knowledge that are needed not simply a list of qualifications which may or may not provide that.

This is particularly the case when some commercial organisations issue 'qualification' certificates based on passing little more than one multiple choice exam. This assessment structure is set up for the purpose of being a cheap marking process not genuine evaluation. The test outcomes struggle to reflect a student's true knowledge and comprehension, as opposed to multiple choice guessing abilities.

Recommendation 1:

Prospective employers and students should pivot toward relying on skills pathways rather than certification-based pathways.

Neither TAFEs nor Universities nor vendors providing short certificates can, in practice, produce cohorts of students who are ready to start a new job without any training by their new employers. It is unrealistic for companies to expect cyber security professionals to be 'job-ready' if they do not have prior experience or the support to develop necessary skills. The cyber security landscape is, as presented, enormously complex. Within each sub-area there are also variations in vendors and internal governance policies, as examples.

Most cyber security jobs require generalist and specialist knowledge, as well as a combination of conceptual and hands-on practical skills. Industry placement experience, through internships, mentoring, in-classroom industry engagement and work experience, can significantly improve the usefulness of new entrants in cyber security jobs to employers. Which, in turn, may reduce the need for inhouse company training. However placement schemes are labor-intensive and expensive to run. Unlike 'instant certificates' passed in a matter of weeks or months, they also take time. Yet, overall they do provide one way that educational institutions can produce better prepared cyber security industry hires.

Employers' cannot expect that 'certificate-qualified' cyber security hires will show up perfectly prepared and exactly in the form that business needs them. Diversifying sources of support beyond Government subsidies and programs is crucial. Encouraging larger corporations that have the resources, to invest in traineeship and apprenticeship programs can significantly contribute to industry development. However, there also needs to be diversification in the training provided so that they are not all based on one vendors' products or methods. Any implementation of a national framework should make this a priority to ensure that Australia does not end up with 'cookie cutter' outputs in our workforce skills. That will not meet the needs of industry nor indeed the needs of the nation which is to have highly diverse skillsets and backgrounds in cyber security.

There is some cause for optimism here. It is significant that the majority of even small to medium sized organisations maintain in-house cyber capabilities. This underscores the fact that some companies of this size are willing to invest in permanent staff rather than outsourcing such services.

Recommendation 2:

Organisations in Australia need to recognise that all new cyber security hires will need training inside their new position.

Cyber security is not 'done' when a program is finished, any more than a government can build a hospital and not maintain it or staff it with skilled doctors. Expanding the number and breadth of strategic government incentives in this area, designed to both bring industry into the classroom and bring the students into industry ahead of course completion, could have a high impact on closing the gap between newly minted cyber security workers and their employers, especially in small to medium sized business. Initial investments in this are a step in the right direction, but may not be enough to meet the growing demand for experienced workers in the near future. It is also important to provide clear mapping across the different educational pathways as a consumer service to students so they can see which learning pathway leads to what professional role they can prepare themselves for. Such clarity of mapping also allows small to medium sized businesses to understand more clearly what skill sets they will find in their new potential hires.

Direct activities are also high value in continuing to close the gap, such as actively organising a spread of small scale, local-community-based hackathons and other hands on training and cyber security engagements. In some cases, these would benefit from clearer articulation of the benefits for participants. It is essential to define specific skill outcomes (and outlining at what proficiency level), along with indicating how these skills can contribute to attaining particular job roles. This approach enhances clarity and enables participants to understand the direct value of engaging in these activities.

Recommendation 3:

There is a very real role for government at a state and national level to expand support for bringing industry and cyber security education providers closer together specifically to build better student outcomes.

Providing this, and keeping it up-to-date, will both highlight the specialist positions where there is demand and make it easier for new entrants, or those transferring from other fields, to better plan their career pathway.

Recommendation 4:

Students and future workers need better, clearer information about the skills and knowledge pathways, so they can make more informed choices.

5. Conclusion

Cyber security skills gaps remain within NSW and Australia. The specific skills gaps that exist within NSW vary according to the size of the organisation and the industry they operate in. There is a disproportionate perception of a gap for AI Security despite limited evidence of real-world experiences of such a gap. Respondents have both identified AI as a solution to the skills gap and a potential generator of new cyber security risk. The messaging around AI in the broader community appears to be creating an impression in some that AI is about to revolutionise the cyber security industry. Evidence supporting that is limited, and whilst there are clear benefits in specific tasks, it remains to be seen whether AI will have the near-term benefit that has been promised.

Cyber security skills gaps remain within NSW and Australia. The specific skills gaps that exist within NSW vary according to the size of the organisation and the industry they operate in. There is a disproportionate perception of a gap for AI Security despite limited evidence of real-world experiences of such a gap. Respondents have both identified AI as a solution to the skills gap and a potential generator of new cyber security risk. The messaging around AI in the broader community appears to be creating an impression in some that AI is about to revolutionise the cyber security industry. Evidence supporting that is limited, and whilst there are clear benefits in specific tasks, it remains to be seen whether AI will have the near-term benefit that has been promised.

Jobs and Skills data indicates a possible softening in shortages for cyber security related jobs, although specialist cyber security jobs continue to see shortages and are predicted to see increases in demand that will exceed the economy-wide average. The AUCyberExplorer data indicates that there are distinct differences between the two major cyber security employment centres (Sydney and Melbourne), including differences in the types of certifications that job openings require. Looking to the future, expansion of government programs to more tightly couple educational organisations and companies in designing and implementing learning experiences would likely assist in closing the skills gap.

There appears to be some confusion or lack of awareness of specific details about the NIST NICE framework from some respondents. Qualitative responses often restated a desire for skills already covered by multiple NIST NICE roles or competencies. Overall, when comparing NIST's NICE framework with similar approaches, for example, the UK's Cyber Security Council's Cyber Career Framework[27], NIST's approach is considerably more complicated. The sheer number of skills and knowledge areas required for each job role may seem at times too complex, particularly for job seekers, students, and small businesses with limited resources.

27 https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/

A more streamlined and approachable framework is desirable if the aim is to encourage new entrants into the field of cyber security. In particular skills pathways that provide a roadmap for those entering further education, and as importantly, those looking to transition into cyber security from other IT specialisms. The plethora of certifications available presents a challenge, with their value difficult to discern and pathways through them hard to define. Cyber security is competing for talent from other IT specialisms and other industries, creating a complicated qualification and certification framework is unlikely to encourage the best and brightest to join.

Future approaches need to be cognisant of the different needs and gaps faced by different industries and organisations of different sizes. A one-size fits all approach is unlikely to deliver optimal returns.

A. Methodology

The survey was conducted during the first three months of 2024. The survey platform provided a total of 736 starts to the survey, with 211 completed. Whilst the completion rate may seem low at just 29%, 325 of the non-completed responses appear to have come from the same device (based on user-agent string matching) and had the same pattern of interaction, very short engagement, typically 10 seconds or less, multiple survey starts within minutes of each other, and all took place between the 2nd and 7th of February 2024. These survey starts may have been caused by automated link checking, or possibly someone checking the survey was live. If we discount them, the completion rate becomes 51%.

The data was evaluated for further cleaning based on time taken to complete the survey. The mean time to complete the survey was a little over fifteen and a half minutes, with a standard deviation a little over twenty five and a half minutes. Consideration was given to removing the responses that took more than 2 standard deviations from the mean but ultimately this was not done. There was doubt about the validity of the time taken field, given that it indicates one respondent had taken 331 minutes to complete the survey. We suspect that if a respondent kept their browser window open it could invalidate the time taken field, and therefore decided to only remove those responses that were marked as incomplete.

Data was extracted from the survey platform and analysed using Python Pandas28 using various methods as described further below.

A.1 Ordinality

We have assumed that the survey responses that involve a likert scale (1-5) should be treated as ordinal data. As such, we have selected non-parametric tests and correlation functions to be consistent with our assumption.

We acknowledge that it is an area of active debate in a number of fields of science as to whether likert data can be treated as continuous or ordinal data. Given our relatively small sample size and the potentially skewed distributions we observed we determined assuming ordinality was the safest option.

When evaluating correlation we have used the Spearman Rank Correlation. When evaluating differences between groups, for example, NSW vs. Other States, a Mann-Whitney U Test was used with the commonplace 0.05 significance level on account of it being a non-parametric test, unlike the more commonplace t-test.

B. Survey results

B.1 NSW vs. Other

When evaluating whether the data from states other than NSW were consistent with the results from NSW it was found that for three questions (competency evaluations) the differences were statistically significant. This section provides graphs for those relevant competencies.

B.1.1 Most Important Competency - Secure Programming

As can be seen from Figure 14 respondents from NSW rated Secure Programming as more important than the rest of Australia. Without further data it is not possible to determine why that is. It could reflect differences in industry participants, for example, greater responses from financial services, the majority of whom consider Secure Programming Very or Extremely important. This can be seen in Figure 15.

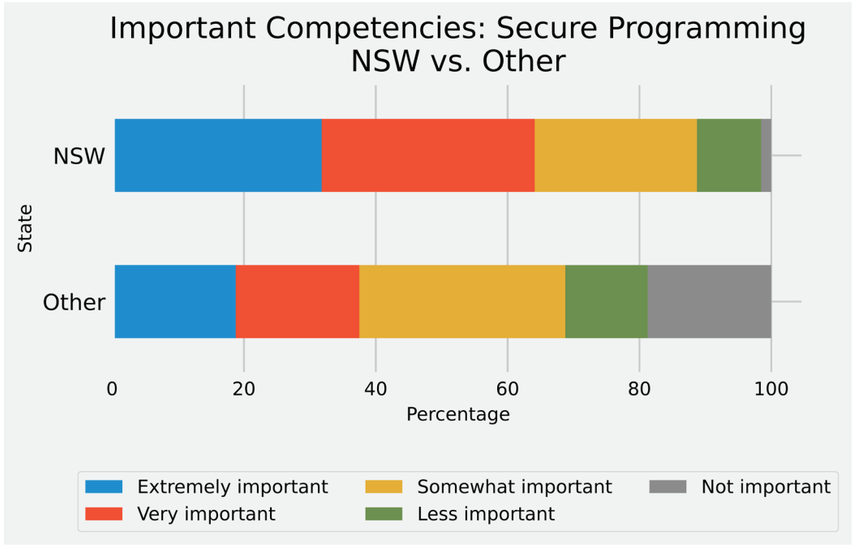

Figure 14: Plot of the Importance of Secure Programming

B.2 Competency Gaps - AI Security

With regards to the question on the biggest competency gaps, again there was a statistically significant difference between the responses from NSW and the rest of Australia, as shown in Figure 16. NSW is rating the gap as larger than the rest of Australia.

If we look at the industry breakdown of the responses, shown in Figure 17, we can again see Financial Services being one of the leading sectors in evaluating the gap to be “Large” or “Extremely large”. This adds to the argument that the discrepancies are due to the different industries that have responded from the various states, which we explore further in Section B.3.1.

B.3 Competency Gaps - Secure Programming

The final competency evaluation that showed statistically significant difference was the Competency Gap associated with Secure Programming. NSW evaluated the gap as being larger than the rest of Australia, as shown in Figure 18. This can be considered consistent with what was described in Section B1.1.

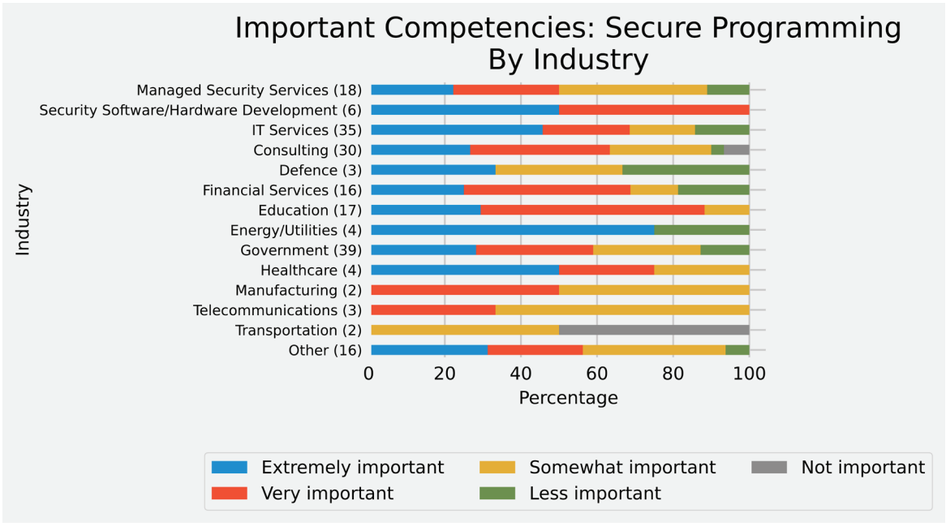

Figure 15: Plot of the Importance of Secure Programming by Industries in NSW

Industry	Responses
Security Software/Hardware Development	1
IT Services	2
Consulting	6
Educating	3
Government	1
Healthcare	1
Telecommunications	1
Other	1

Table 2: Respondent Industries Outside of NSW

B.3.1 Industry Breakdown

Exploring the breakdown of industries further, we can see from Figure 19 that NSW has a broad range of industry representation, with the majority coming from IT Services, Government and Consulting, but still with reasonable representations from Financial Services, Managed Security Services, and Education. By contrast, the rest of Australia has a more limited industry representation, with no responses from Financial Services or Managed Security Services, amongst others. However, it should be noted that the sample size from outside of NSW is limited at only 16, with absolute breakdowns of industries provided in Table 2.

B.4 Additional Plots

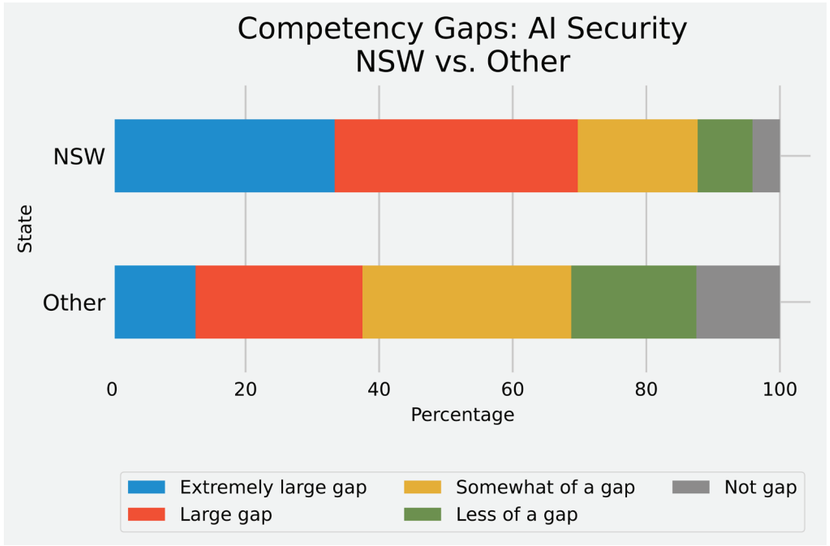

Figure 16: Plot of the Competency Gaps Evaluation for AI Security

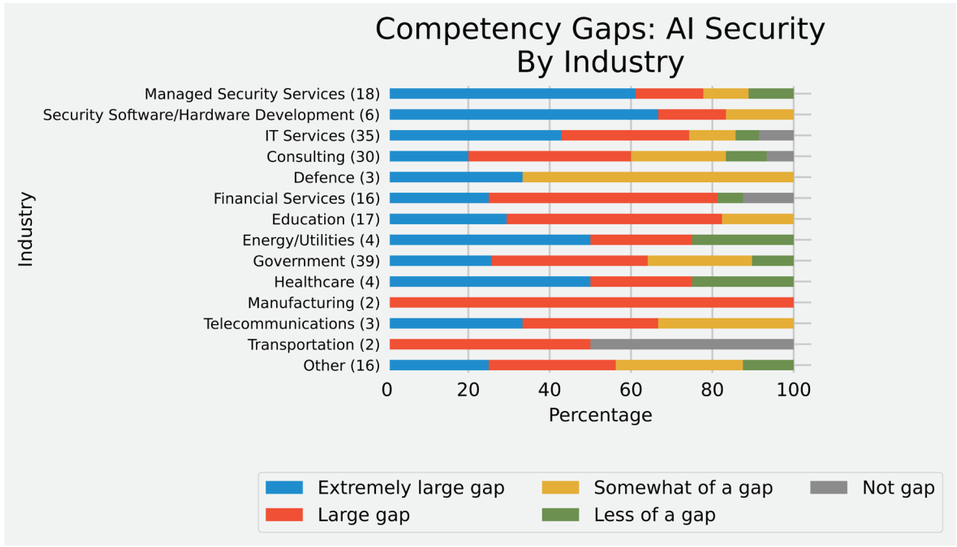

Figure 17: Plot of the Competency Gaps Evaluation for Secure Programming by Industries in NSW

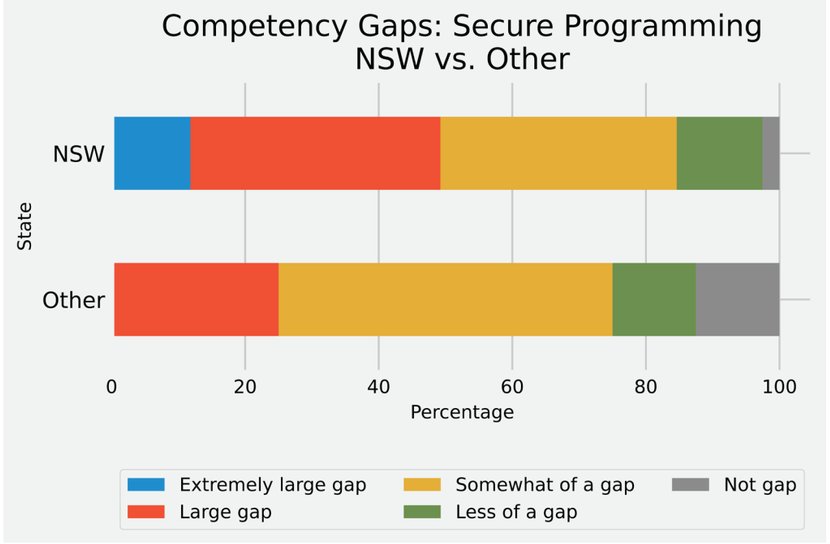

Figure 18: Plot of the Competency Gaps Evaluation for Secure Programming

B.4 Additional Plots continued

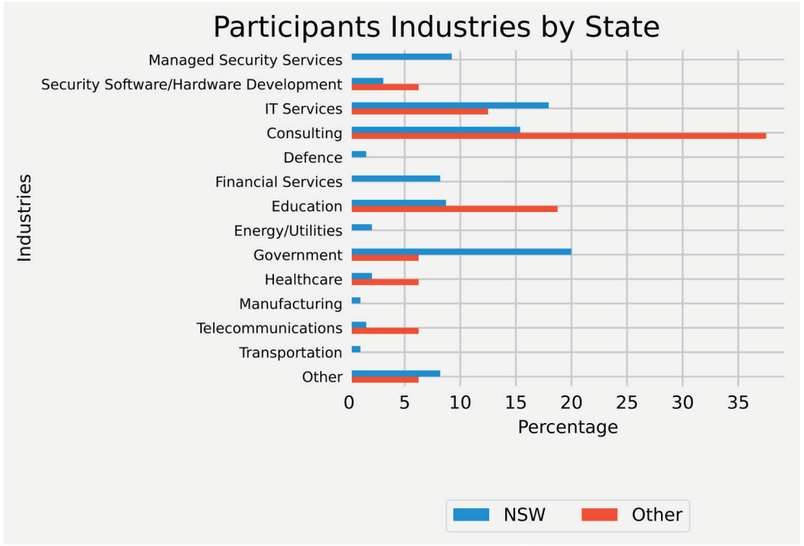

Figure 19: Plot of Participants Industries by State (NSW or Other)

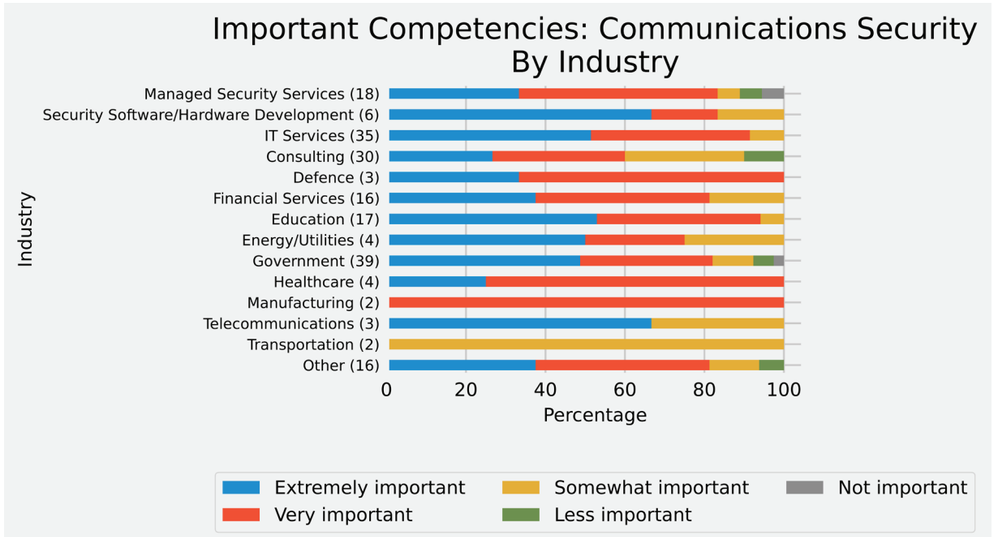

Figure 20: Plot of the Importance of Communication Security by Industries in NSW

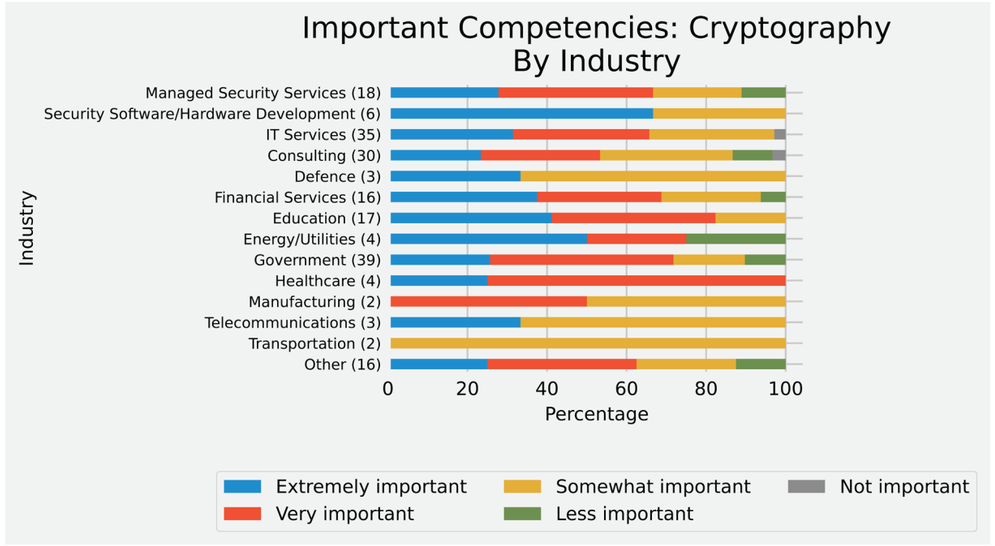

Figure 21: Plot of the Importance of Cryptography by Industries in NSW

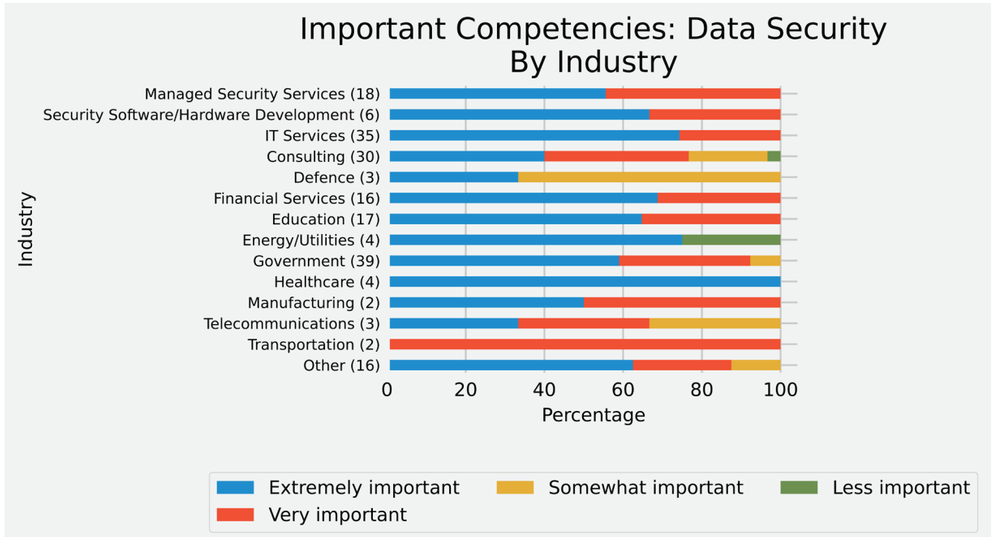

Figure 22: Plot of the Importance of Data Security by Industries in NSW

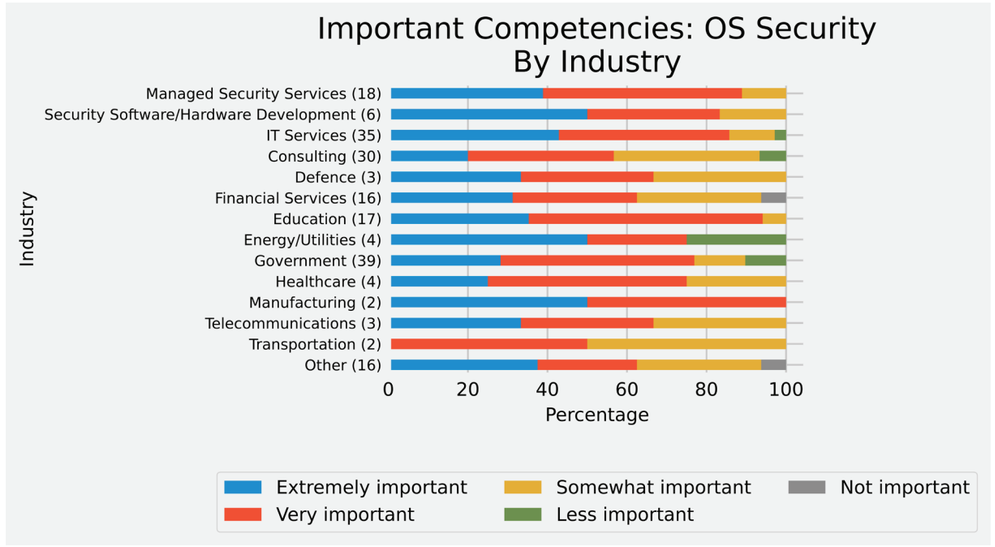

Figure 23: Plot of the Importance of OS Security by Industries in NSW

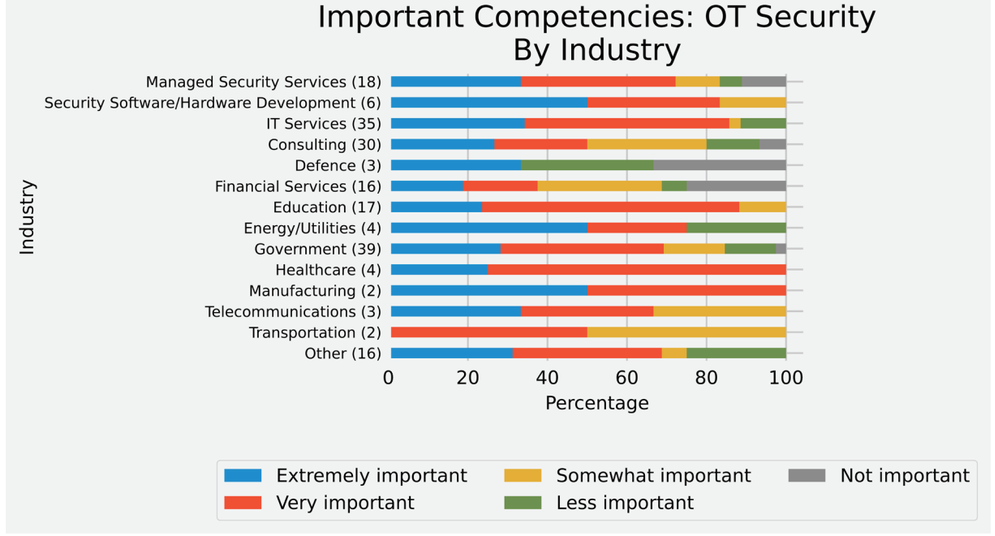

Figure 24: Plot of the Importance of OT Security by Industries in NSW

Figure 25: Size of Organisation Impact on Perceived Competency Gap

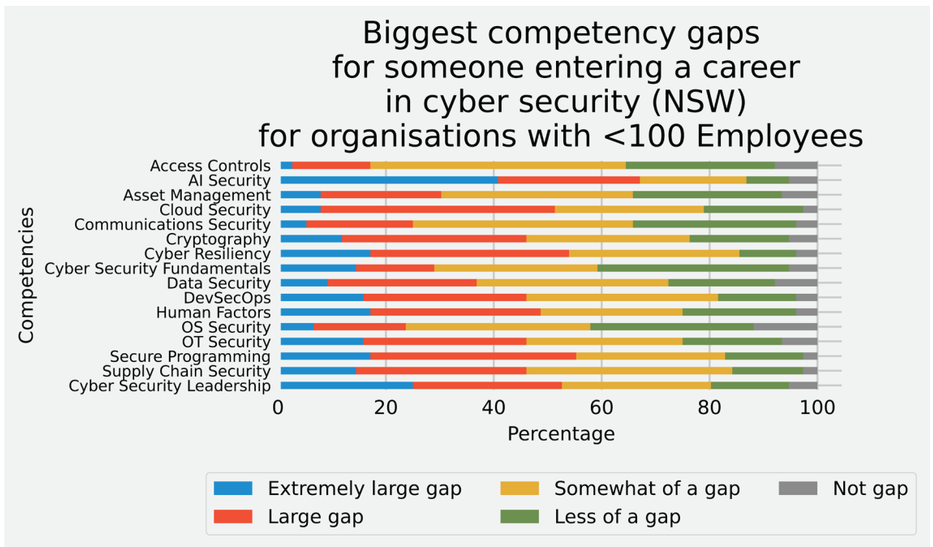

Figure 25a: Comptency gaps from organisations with <100 employees

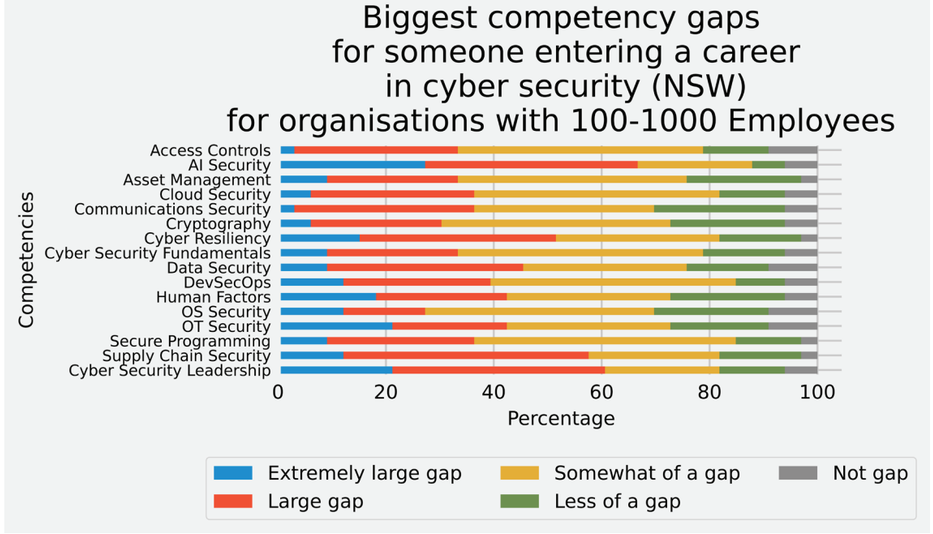

Figure 25b: Competency gaps from organisations with 100-1000 employees

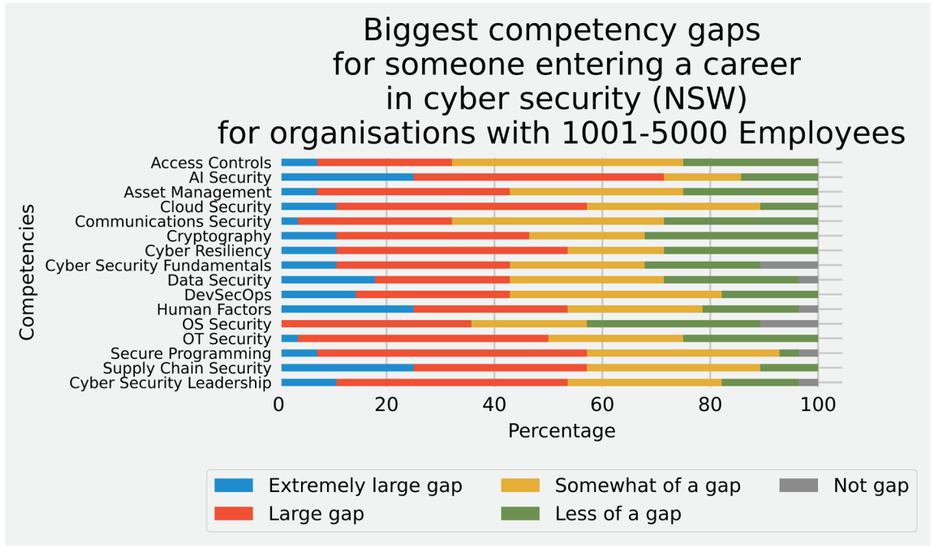

Figure 25c: Competency gaps from organisations with 1001-5000 employees

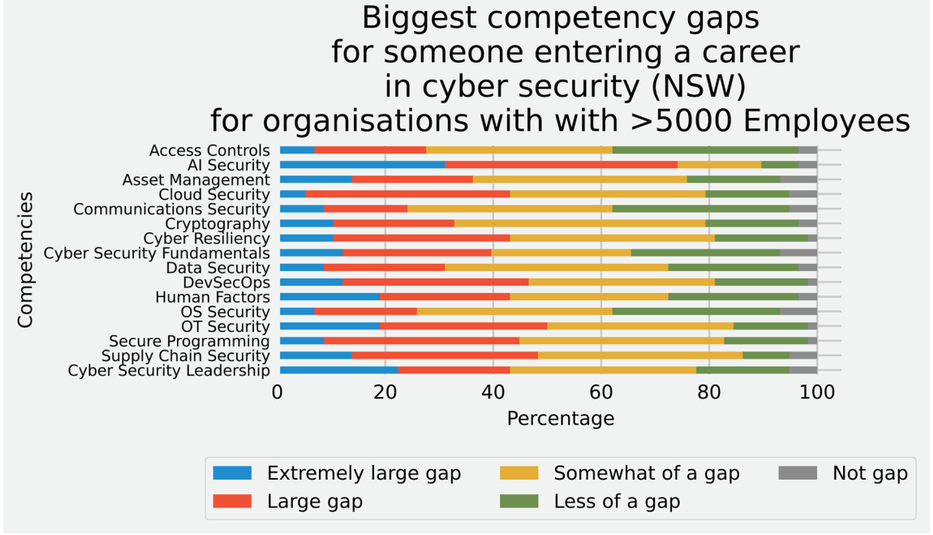

Figure 25d: Competency gaps from organisations with >5000 employees

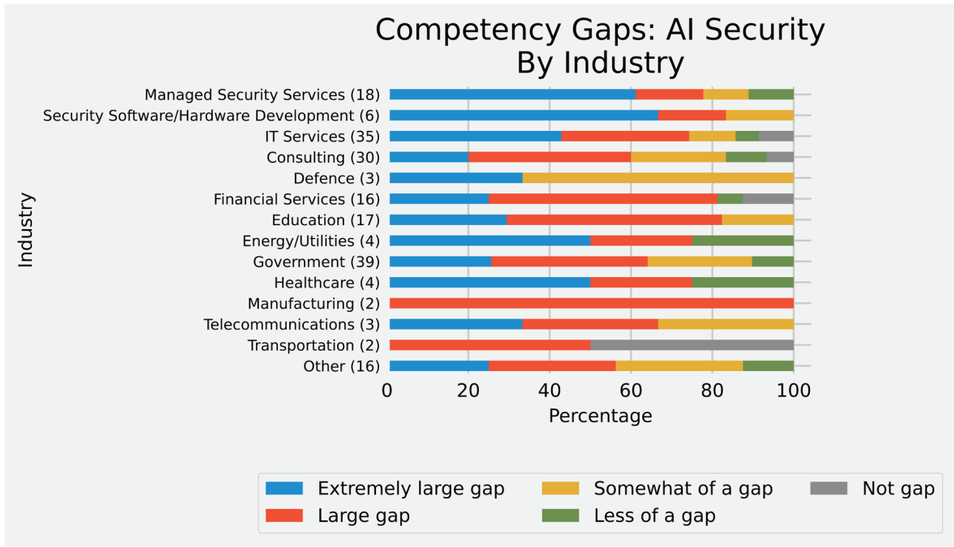

Figure 26: Plot of the Perceived Gap for AI Security by Industries in NSW

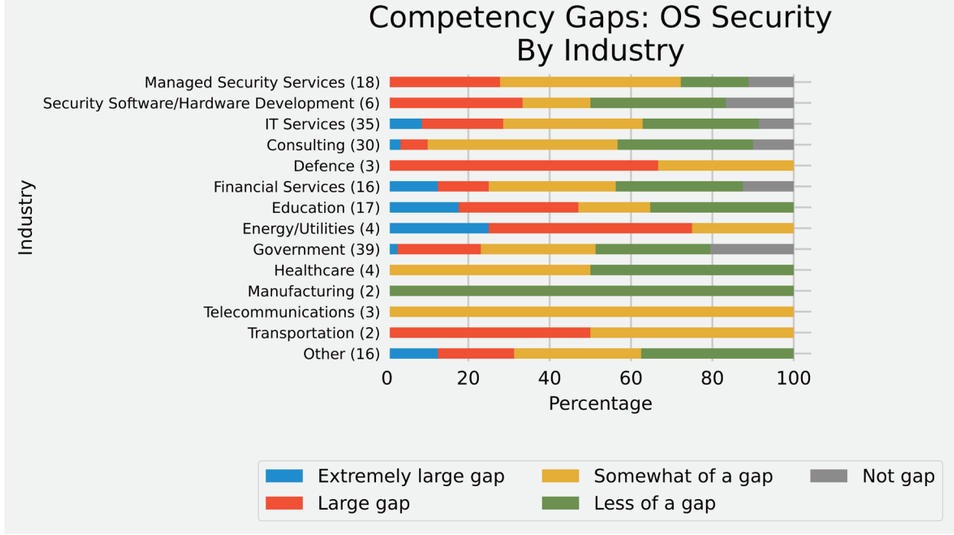

Figure 27: Plot of the Perceived Gap for OS Security by Industries in NSW

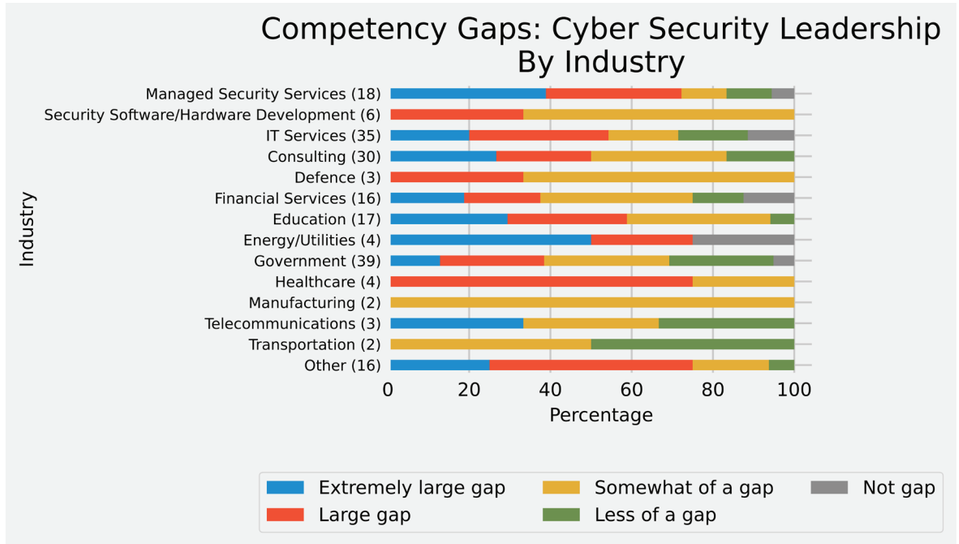

Figure 28: Plot of the Perceived Gap for Cyber Security Leadership by Industries in NSW

The NSW Cyber Business Exchange is a NSW Government Funded Program

AISA

Australian Information Security Association