

# LITERATURE REVIEW

Investigating factors influencing  
the attrition of women in the cyber  
security workforce

Prepared for:



# AUTHORS

Associate Professor Lena Wang

Associate Professor Lauren Gurrieri

Dr Salvatore Ferraro

Dr Maria Beamond

Dr Amy Corman

We also acknowledge the work of  
Karthika Kumar and Dr Bronwyn Bruce.

# TABLE OF CONTENTS

**04**

Executive summary

**07**

1. Introduction

**10**

2. The Australian cyber security workforce

**14**

3. Gender inequality statistics in cyber security and STEM disciplines internationally

**18**

4. Barriers to gender diversity and inclusion in cyber security

**25**

5. Enablers of gender diversity and inclusion in cyber security

**33**

6. Conclusion

**35**

References



# EXECUTIVE SUMMARY

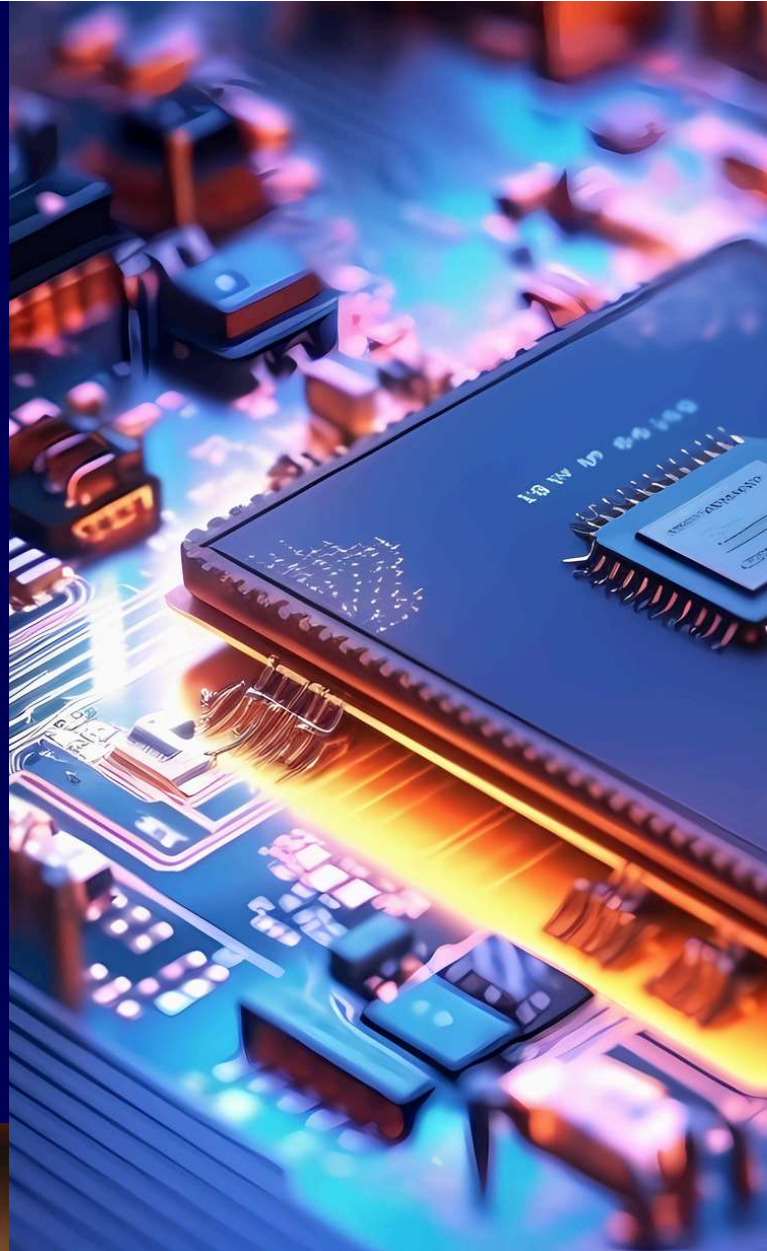
In response to growing social and political pressures to demonstrate diversity, equity and inclusion, organisations are focusing on redesigning internal practices and processes that foster greater workplace gender equality. Cyber security remains a heavily male dominated profession in Australia (Risse et al., 2023) and internationally (ISC2, 2023). There is urgency to address persistent workplace gendered inequities given realised and projected strong growth in demand for cyber security professionals (Department of Home Affairs, 2023; OECD, 2023) and the challenges associated in recruiting this cohort (Crumpler & Lewis, 2022).

Sponsored by the Australian Signals Directorate (ASD), the Australian Women Security Network (AWSN) has commissioned RMIT University's Centre for Cyber Security Research and Innovation (CCSRI) and Centre for Organisations and Social Change (COSOC) to undertake Phase II of a research project focusing on female cyber security professionals in Australia. The objective of Phase II is to document and explore the reasons for the under-representation of women in Australia's cyber security workforce and to develop a set of policies and initiatives designed to improve gender diversity and inclusion. The overarching goal of this research is to ensure that the Australian cyber security workforce is able to meet the growing demand for cyber security services from the public, business, and household sectors.

Completed in 2023, Phase I of the research project included a review of the literature on the cyber security workforce, an exploration of the latest Australian Census from 2021, and quantitative analysis of an online survey. The Census analysis revealed that women account for 17 percent of the cyber security workforce in Australia (Risse et al., 2023), which is broadly in line with international trends (ISC2, 2018). Responses from an online survey of over 700 female and male cyber security professionals highlighted various gendered barriers in cyber security, including a notable lack of female role models in the profession (Risse et al., 2023).

Phase II of the research project includes a qualitative research design to investigate the underlying factors contributing to women's low participation in, and departure from, Australia's cyber security workforce. The research objectives of the current phase are to:

- Develop a deep understanding of the multi-faceted reasons as to why women leave the cyber security profession.
- Gain insights into the lived experiences of women in the cyber security sector, focusing on challenges and opportunities for improvement.
- Explore the potential interventions and strategies that organisations may implement to enhance gender diversity and retention of women in the cyber security workforce.



The methodology for Phase II is comprised of three stages:

1. A literature review of gendered enablers and barriers in the cyber security workforce.
2. In-depth interviews with 30 women currently working in cyber security roles with over five years of experience, or those who have recently left the cyber security workforce.
3. Thematic analysis of interviews of women currently working, or who have worked, in cyber security roles.

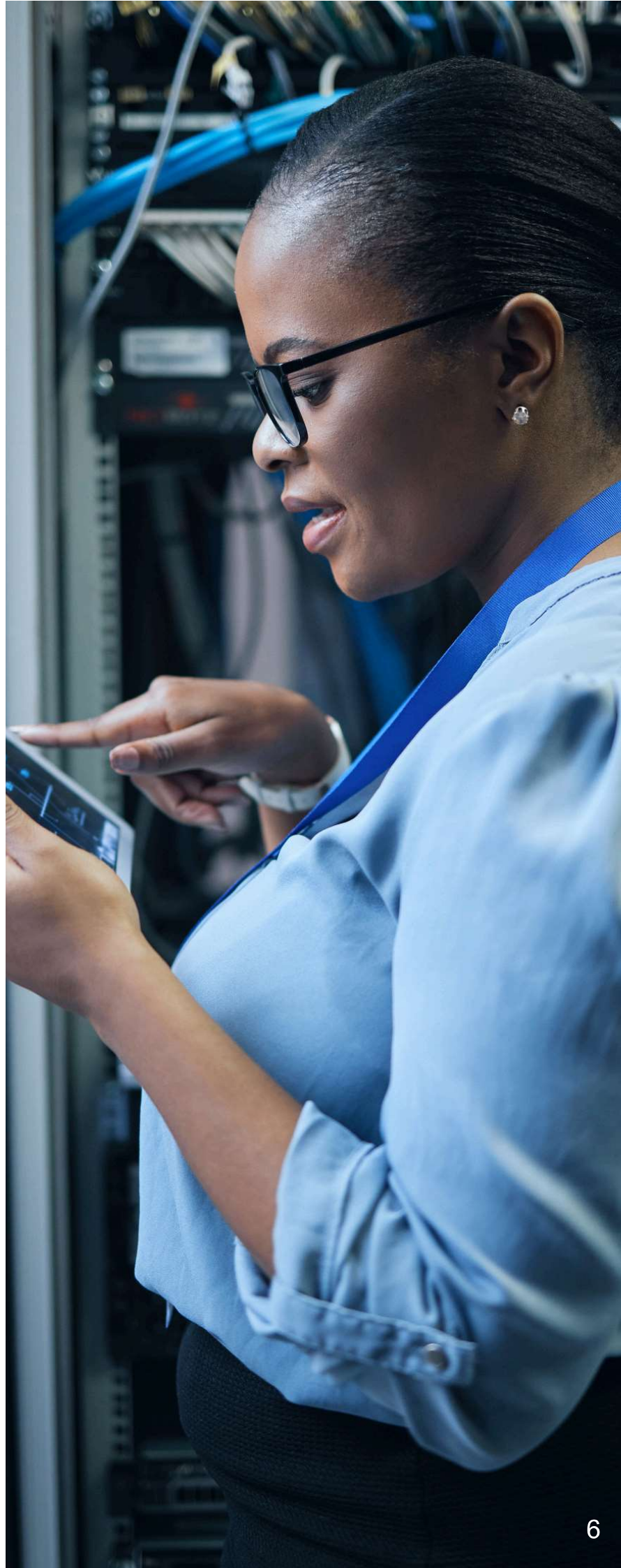
Building on the literature review completed in Phase I, this report represents the first stage of Phase II, focusing on an in-depth review of more up-to-date literature that explores two key areas:

- Examination of gendered barriers that may contribute to problems around recruitment and retention of women in cyber security.
- Policy recommendations designed to improve gender diversity and inclusion in cyber security.

The report provides a foundation for the research and highlights gaps in current knowledge.

Combined with the key findings from the lived experiences of women in the cyber security workforce and those who have left, Phase II of the research project makes the following contributions:

- It addresses the current and future professional skills shortage in the cyber security industry by evaluating the factors that influence attrition of women in the cyber security workforce.
- It identifies how enablers and barriers relate to broader cultural factors and institutional practices can be shaped by changes in workplace policies and strategic interventions by key agencies and stakeholders, in order to support women's retention, attraction and management.




# 1. INTRODUCTION

Australia, amongst many other nations, still has a long way to go in achieving gender equality in STEM disciplines, with women accounting for only 15 percent of STEM-qualified occupations but half of non-STEM occupations as of 2022 (Department of Industry, Science and Resources, 2023). Existing research attributes this low female representation to a variety of factors, such as masculine cultures that reduce women's sense of belonging, limited early exposure to these disciplines, and a lack of confidence or self-efficacy (Cheryan et al., 2017). Further, because women are subject to additional domestic workloads and take on the lion's share of child rearing responsibilities, they may face challenges pursuing and maintaining STEM careers (Cech & Blair-Loy, 2019; Prieto-Rodriguez et al., 2022). These struggles in maintaining STEM careers have also been noted by Glass et al. (2013), who demonstrated that women in STEM fields are significantly more likely to leave their occupational fields compared to those in non-STEM fields.

Given that many cyber security professionals have educational and/or professional backgrounds in computer/information systems and IT (Foley et al., 2017), it is not surprising that cyber security remains male dominated. Research reveals that in Australia and internationally, less than one in five cyber security professionals are women (ISC2, 2023; Risse et al., 2023).[1] Challenges in recruiting qualified and experienced cyber security professionals however are also rising, as the talent pool struggles to keep up with the growth of demand (Crumpler & Lewis, 2022). Consequently, lifting female participation in cyber security may be a means to address these shortages.

Since low female representation in cyber security and STEM occupations can reflect problems around the recruitment and retention of women, attrition of women has naturally been identified as an avenue for investigation (ACS (2015; McIver, 2022). This idea is supported by research which shows that in the United States, women in STEM occupations are more likely to leave their occupational field than other professional women, particularly early in their career (Glass et al., 2013). Moreover, according to the 2022 (ISC2) Cyber Security Workforce Study, 60 percent of cyber security enterprises have had difficulty in retaining workers, with staff turnover rates of around 20 percent in the workforce overall.

[1] For the Australian estimate, five occupational categories make up cyber security (cyber security) roles, as per the Australian & New Zealand Standard Classification of Occupations (ANZSCO): cyber security advice and assessment specialists, cyber security analyst, cyber security operations co-ordinator, cyber security architect, and cyber governance risk and compliance specialist. The Census relies on respondents to accurately self-report the occupational category they belong to, as well as other professional and personal characteristics. The ISC2's estimate of the global cyber security workforce is primarily based on survey based estimates for the United States which are used as a baseline for the rest of the world.



Our review of the relevant literature suggests that there are limited studies which investigate or document low retention of women working in cyber security. This may reflect that much of the research is based on surveys of cyber security professionals at one point in time rather than longitudinal surveys that track the workforce dynamics across time. Added to this, studies on gender disparities in Australia's cyber security workforce are sparse.

Given the scarcity of studies that investigate gendered disparities in the Australian cyber security workforce, our report draws on the wider literature in STEM occupations to leverage insights that have already been developed in related occupational categories.

This then leads us to the aim of this report, which is to enhance our overall understanding of gender equality in the Australian cyber security profession with a view to offering solutions to reduce gender disparities. The report is structured as follows.

In **Section 2** we review the limited number of studies that have examined the Australian cyber security workforce, including the key findings from Risse et al. (2023) which comprised Phase I of this project.

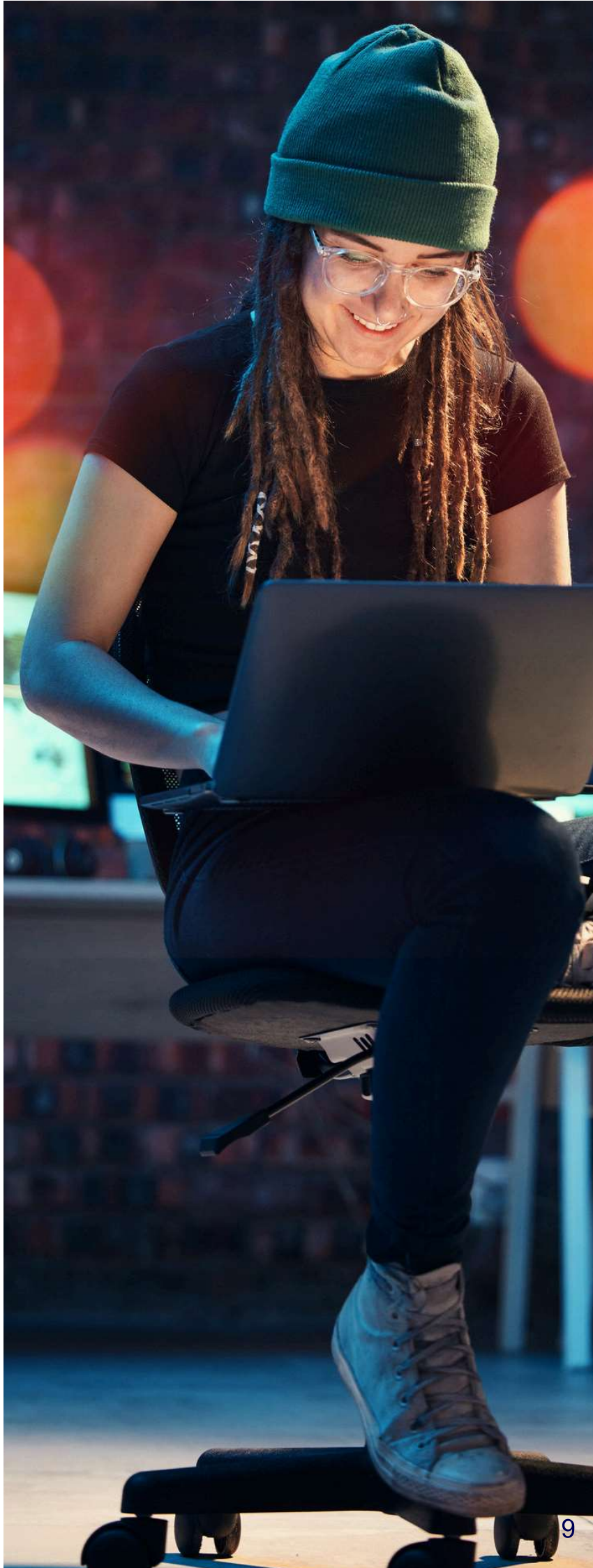
In **Section 3** we aim to establish quantitative and statistical support for the presence of gendered barriers in cyber security. While research is suggestive of female under-representation and other gender inequalities in cyber security, some of these studies are based on surveys that exhibit low response rates, small samples and selection bias that may distort and reduce the external validity of their findings (Bethlehem, 2010). We therefore report summary statistics on measures of gender inequality in cyber security and related STEM occupations both in Australia and internationally. The focus is on data collected by statistical bureaus that are based on large samples of non-voluntary participants which mitigates the problem of selection bias.



Consistent with international trends, evidence of low female representation in cyber security in Australia is pervasive across different activities and levels of seniority, and a sizeable gender pay gap in the profession persists. In addition, workplace gender disparities can manifest in ways that are difficult to measure statistically and systematically. These include harassment and professional micro-aggressions that can arise from unconscious bias and masculine cultures.

Consequently, in **Section 4** we explore the organisational and societal factors that contribute to gender disparities in cyber security, including job design unique to cyber security and other STEM occupations, the prevalence of a hyper-masculine culture that is reflected in the language used to describe and promote the profession, and a lack of a support network for female cyber security professionals (LeClair & Pheils, 2016; Peacock & Irons, 2017).

In **Section 5** we canvas policies and initiatives designed to support efforts to improve gender diversity and inclusion in cyber security. These include recruitment enablers such as gender targets, changes to job design that promote a cultural shift away from being available 24/7, fostering a gender inclusive culture, and supporting women's career progression opportunities through various initiatives, including the development of mentoring networks. In **Section 6** we conclude this report and discuss avenues for future research in this area.



# 2. THE AUSTRALIAN CYBER SECURITY WORKFORCE

## 2.1 Gender dimensions of Australia’s cyber security profession (Phase I of this research)

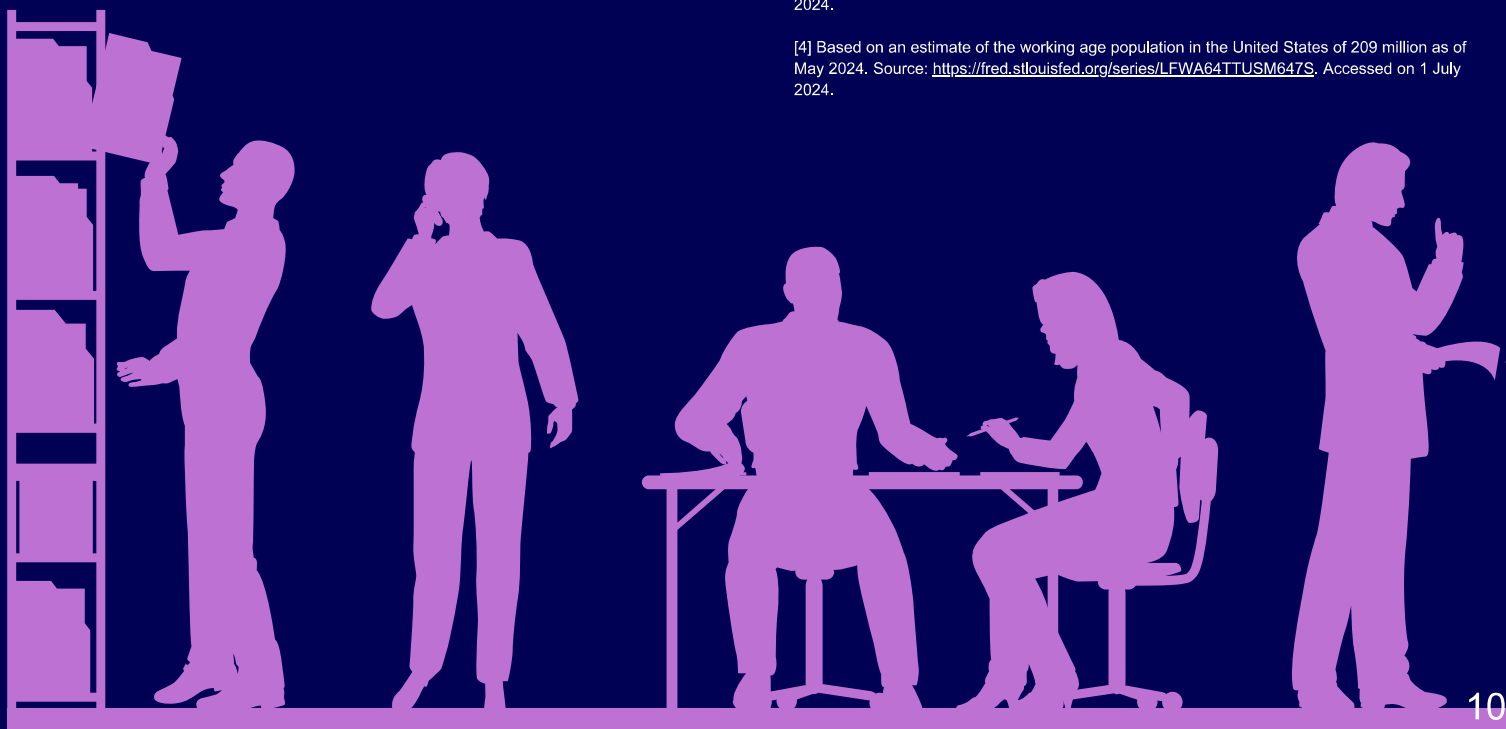
Based on an analysis of the recently developed occupational categories for cyber security professionals by the Australian Bureau of Statistics, Phase I of the research project demonstrated that Australia’s cyber security workforce is heavily male dominated. To our knowledge, the quantitative analysis undertaken in Phase I was the first of its kind to identify and measure the size of Australia’s cyber security workforce conditioned by gender from population data rather than from the gender composition of survey responses (ISC2, 2023) which typically have low response rates and can be subject to selection bias, hence resulting in potentially unrepresentative findings (Bethlehem, 2010). Phase I also included an online survey of cyber security professionals which pointed to a lack of female role models and associated gender disparity in senior leadership positions (Risse et al., 2023).

The under-representation of women in cyber security is in line with the pattern in the broader occupational category of IT Professionals, where the female share is around 21%.<sup>[2]</sup> Prior to the latest Census, cyber security professionals were mainly counted in the ICT Security Specialist category which shows growth of over 200 percent between 2016 and 2021, with the female share of the 13,300 professionals in this workforce of around 16 percent as of 2021 (Risse et al., 2023). To put the size of Australia’s cyber security workforce – which is 0.1 percent of the working age population<sup>[3]</sup> – in a global context, the Bureau of Labour Statistics reports that the number of full-time workers in the occupational category Information Security Analysts in the United States was 145,000 as of 2021 (BLS, 2024) or 0.1 percent of the working age population.<sup>[4]</sup>

<sup>[2]</sup> Calculated by the authors from the 2021 Census retrieved from ABS Pro Table Builder on 8 June 2024.

<sup>[3]</sup> Based on an estimate of the working age population in Australia of 16.9 million as of 2022. Source: <https://data.oecd.org/pop/working-age-population.htm#indicator-chart>. Accessed on 1 July 2024.

<sup>[4]</sup> Based on an estimate of the working age population in the United States of 209 million as of May 2024. Source: <https://fred.stlouisfed.org/series/LFWA64TTUSM647S>. Accessed on 1 July 2024.



# 10%

**C-suite roles**

This under-representation of women in Australia's cyber security workforce extends to senior leadership positions. Of the 510 female cyber security professionals participating in the online survey of Phase I, only 10 percent of female respondents were employed in C-suite roles such as Chief Executive Officers, Chief Financial Officers and Chief Information Officers (i.e. most senior leaders within their organisations) compared to 20 percent of male respondents, although gender composition of senior management positions (i.e. a level lower than C-suite executive roles) was comparable (Risse et al., 2023).

# 29%

**Have a mentor**

Research shows that 29 percent of female cyber security professionals reported having a mentor of the same gender compared to half of male cyber security professionals (Risse et al., 2023). They also reported being more motivated than men by the impact of their work on the community, with 52 percent of female respondents as opposed to 44 percent of men reporting a desire to work in a profession which makes a difference to society. Women also perceive their skill set being under-utilised, with only 35 percent of female respondents saying that their profession offers the opportunity to use their skills compared to 44 percent of men (Risse et al., 2023).

# 52%

**Want to make a difference to society**

Lastly, the factors that were seen to most promote career progression among both male and female respondents were on-the-job learning, informal networks, mentoring, and professional development courses. The current state of organisational initiatives to foster gender equality was seen to be largely ineffective, with less than one in five respondents reporting that they had benefited from organisational initiatives to foster gender equity (Risse et al., 2023).

# 35%

**Have the opportunity to use their skills**

## 2.2 Other studies of Australia's cyber security workforce

The few existing studies of Australia's cyber security workforce focus on the need to facilitate more diverse representation (Department of Home Affairs, 2023), the skills sought by employers (Potter & Vickers, 2015), and the barriers facing women specifically, particularly the low enrolment by school aged girls in cyber security tertiary courses (Bongiovanni & Gale, 2023).

The Australian Government has identified that Australia's cyber security profession exhibits skills shortages with low representation from women and other diverse groups (Department of Home Affairs, 2023). It proposes to continue to incorporate cyber security teaching within schools, develop a nationally recognised cyber security accreditation, and consult with industry to devise strategies that expand the diversity of the workforce, including the representation of women (Department of Home Affairs, 2023).

Potter and Vickers (2015) have undertaken a non-gendered analysis of the demand for certain types of cyber security skills in Australia, based on skills sought by employers in job listings and interviews with cyber security professionals. It was found that there was a common set of 'hard' skills desired across different roles – including experience, qualifications and technical expertise – and 'soft' skills – including relationship management and leadership (Potter & Vickers, 2015).

The study by Bongiovanni and Gale (2023) of the barriers facing women in Australia's cyber security workforce are based on an analysis of enrolments into university level cyber security programs and interviews of cyber security professionals, undergraduates and HR managers. Three key barriers identified by Bongiovanni and Gale (2023) include:

- The perception that cyber security roles are predominantly technical.
- The masculinised culture associated with the profession being male dominated.
- The fact that women are not encouraged to pursue a career in cyber security.

Given the study includes interviews of men and women, as well as Human Resources managers, it does not exclusively draw on the lived experiences of women working in cyber security, the gendered barriers they have encountered, and how these barriers have been navigated.

## 2.3 Summary

The literature which investigates gender dimensions in Australia's cyber security workforce is limited, which might reflect in part the fact the occupational category is a relatively contemporary one. Existing studies confirm that the profession in Australia remains male dominated (Risse et al., 2023) and that gendered barriers include both gendered stereotypes about the field which discourages women from pursuing careers in the field, and the persistence of a masculinised culture (Bongiovanni & Gale, 2023).



# 3. GENDER INEQUALITY STATISTICS IN CYBERSECURITY AND STEM DISCIPLINES INTERNATIONALLY

In addition to the findings reported in Phase I, we have expanded our review to document additional dimensions of gender disparity – in terms of workforce composition and pay gaps – for Australia and internationally both in the cyber security profession and related STEM disciplines. Most of the international statistics reported below on cyber security are focussed on the United States due to lack of data availability for other countries. In summary, the data shows that the under-representation of women in cyber security and related fields in Australia is consistent with international patterns. In Australia, the gender disparity extends to managerial positions and a sorting of women into lower paid administrative roles which likely contribute to evidence of a sizeable gender pay gap.

## 3.1 Gender composition

### 3.1.1 Under-representation of women

Although international estimates of the female share of the cyber security workforce are based on survey response rates – participation in which is voluntary – the under-representation of female cyber security professionals evident in Australia appears to be consistent with international evidence. Based on several surveys, ISC2 estimates

that the female share of global cyber security professionals varies from 16 percent (ISC2, 2023) to 24 percent (ISC2, 2018). For the occupational category of Information Security Analysts in the United States, the estimated count of 26,000 women accounts for less than 20 percent of the total workers in this category of 145,000 as of 2021.[5]

This under-representation of women in cyber security extends to the closely related IT and STEM disciplines. Less than 30 percent of the employed STEM-qualified workforce in Australia is comprised of women, while women account for only 25 percent of the information and communications technology workforce (Professionals Australia, 2017). The share of women in IT occupations in the United States declined to 25 percent in 2014 from 31 percent in 1990 (Beckhusen, 2016).

From an historical perspective, War World II (1939-1945) represents an exception to the pattern of under-representation of women in cyber security and information systems. During this period, around 11,000 women were recruited by the Army and Navy of the United States as intelligence code breakers, accounting for more than half of the code breakers enlisted in the defence forces (Mundy, 2017).

[5] Based on the authors' own calculations from data accessed on 10 June 2024. <https://www.bls.gov/opub/reports/womens-earnings/2021/home.htm>.

### 3.1.2 Women in leadership

Vertical segregation, the imbalance between women and men in leadership categories, describes the structural disadvantage faced by women that leads to limited opportunities for career progression and low representation in senior managerial and leadership roles (Professionals Australia, 2017). Vertical segregation is evident in the cyber security workforce in Australia with a considerably higher share of male survey respondents holding C-suite executive roles (Risse et al., 2023). Similarly, in the United Kingdom, less than 15 percent of senior roles in cyber security were held by women as of 2022 (Coutinho et al., 2023).

This pattern is also seen in the Australian 2021 Census data for the ICT profession more broadly, where women account for less than 25 percent of ICT managers - comprised mainly of ICT Project Managers and Chief Information Officers - considerably lower than the female share of the Managers across all occupational categories of 40 percent.[6]

### 3.1.3 Horizontal gendered segregation

Gendered segregation in the workplace represents one of the manifestations of gender inequality in organisations (Cohen, 2013). Horizontal segregation is defined as women and men sorting into different types of work activities, with women being employed typically into more precarious forms of employment such as part-time and casual positions compared to men (Professionals Australia, 2017).

There is evidence that among ICT professionals in Australia, women are more likely to be employed in more junior and therefore lower paid administrative and logistical support roles (Foley et al., 2017). Based on the Australian 2021 Census, 17 percent of the women in the Computer System Design and Related Services industry are classified as Clerical and Administrative Workers compared to two percent of men[7].

### 3.2 Gender pay gap

The gender pay gap is sizeable and persists across cyber security and related disciplines in Australia. Based on the latest data available in the 2021 Australian Census, the median personal weekly income for women in the ICT Security Specialists occupational category was between \$1,750 and \$1,999 compared to a range of \$2,000 and \$2,499 for men, amounting to a gender pay gap of 12 percent to 25 percent. [8] The gender pay gap likely reflects the gender composition of the cyber security workforce, notably horizontal segregation and lack of female leaders in the profession.



[6] Calculated by the authors from the 2021 Census retrieved from ABS Pro Table Builder on 8 June 2024. Female ICT Managers number 17,602 from a total of 74,540 ICT Managers. For the Managers category, female Managers number 652,412 from a total of 1,645,769 Managers.

[7] Calculated by the authors from the 2021 Census retrieved from ABS Pro Table Builder on 8 June 2024. The ABS classifies this industry as workers 'engaged in providing expertise in the field of information technologies such as writing, modifying, testing or supporting software to meet the needs of a particular consumer; or planning and designing computer systems that integrate computer hardware, software and communication technologies.' Source: <https://www.abs.gov.au/statistics/classifications/australian-and-new-zealand-standard-industrial-classification-anzsic/2006-revision-2-0/detailed-classification/m/70/700/7000>. Accessed on 1 July 2024.

[8] The gender pay gap is expressed as the median women's weekly earnings as a percentage of the median men's weekly earnings. The median weekly incomes that form the basis of the gender pay gap estimate do not take into account differences in employment status or weekly hours worked between women and men. Based on the authors' own calculations using data accessed from the ABS Pro Table Builder on 10 June 2024.

The gender pay gap is pervasive across the STEM disciplines that effectively supply workers into cyber security. Measured by full-time total remuneration, the Department of Industry, Science and Technology estimates that men earned an average 15 percent more than women in the Computer System Design and Related Services industry as of 2022, comparable to the gender pay gap for all STEM industries (Department of Industry, Science and Resources, 2023) and within the range of estimates for the gender pay gap for Australia's economy wide workforce of 12 percent to 22 percent.

Based on an analysis of survey respondents from Australia, around 40 percent of female professionals in STEM believed that their pay was not fair or equitable compared to their professional male colleagues and survey respondents ranked pay equity behind only flexible work arrangements as a key barrier to career advancement facing professional women (Professionals Australia, 2017). Added to this, the gender pay gap widens considerably for female engineers with more than four years of industry experience, pointing to the role that career interruptions play in propagating pay disparities between women and men (Professionals Australia, 2017).

International patterns point to a modestly lower gender pay gap than in Australia. In a global survey of cyber security professionals, the average annual salary for female participants was \$109,609 compared to \$115,003 for male participants, amounting to a gender pay gap of around five percent (ISC2, 2024).

# 15%

**Gender pay gap between men and women in Computer System Design in Australia**

# 12-22%

**Gender pay gap for ICT security specialist roles in Australia**

# 5%

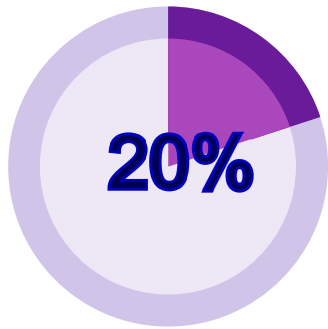
**Gender pay gap between male and female engineers internationally**



### 3.3 Summary

Drawing on statistics primarily collected for Australia and the United States, our empirical analysis confirms that women account for less than one in five cyber security professionals, that this low female representation extends to leadership positions, and that gendered workplace segregation is present in STEM occupations more broadly, where women are over-represented in administrative and clerical roles that are characterised by low pay (see Figure 1). These factors are likely to contribute to the sizeable gender pay gap which we find evidence for in Australia both in cyber security and related STEM occupations. Since the low representation of women in cyber security and STEM occupations does not appear to be Australia-specific, the underlying gendered barriers in the profession are likely to be global in nature, which will be discussed in Section 4.

**Figure 1:** Gender disparities in cyber security and related occupations in Australia



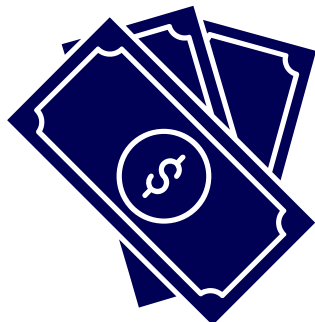
**Women account for less than 20% of Australia's cyber security workforce**



**Less than 25% of ICT project managers and chief information officers are women**



**One in five women in the computer system design and related service industry are classified as clerical/administrative workers, compared to one in 50 for men**



**Women working as ICT security specialists earn 12-25% less than their male counterparts**

# 4. BARRIERS TO GENDER DIVERSITY AND INCLUSION IN CYBER SECURITY

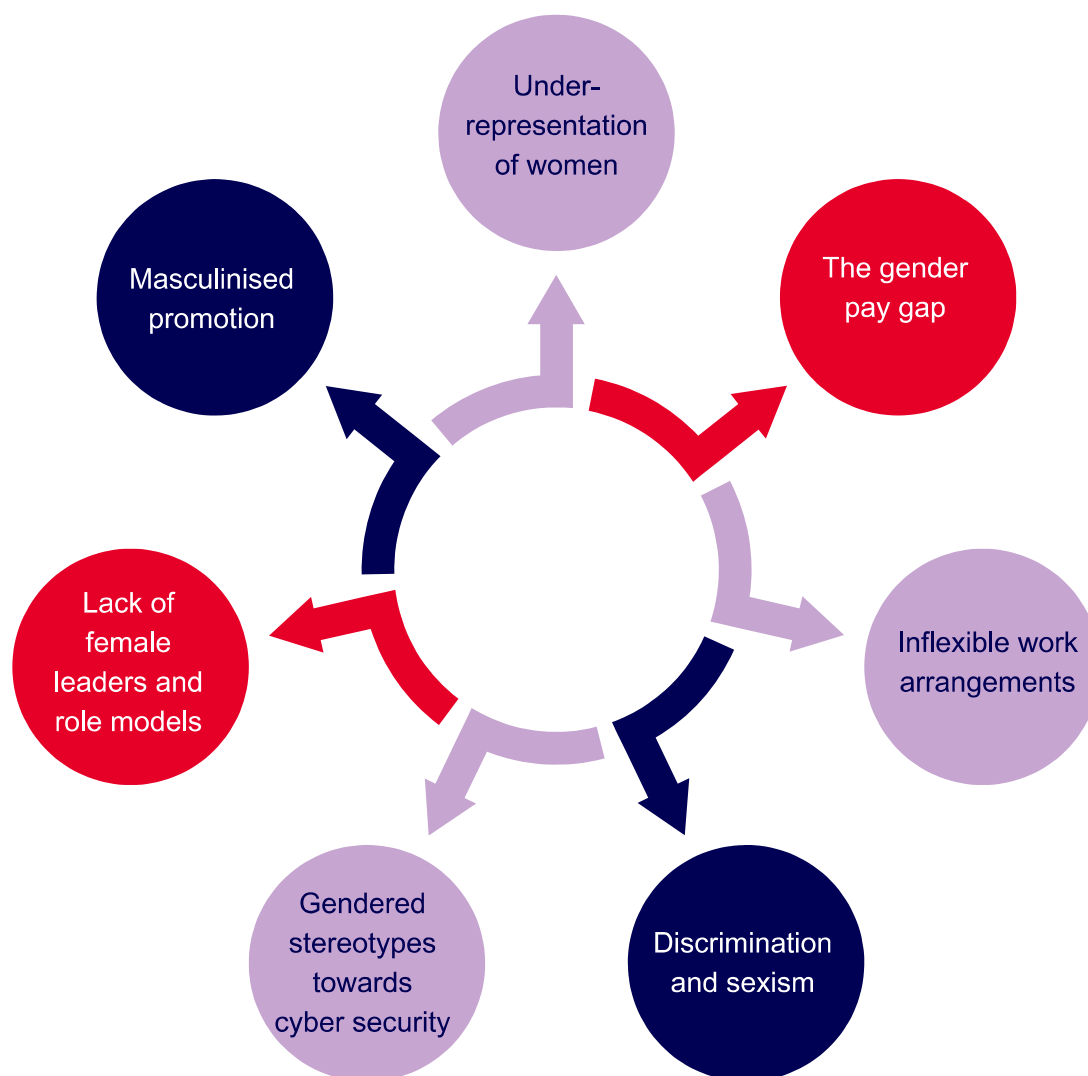
Our discussion of gendered barriers in the workplace focuses on both the lack of gender diversity and inclusion. Although diversity and inclusion are often thought of as being interchangeable, they represent distinct concepts (Garg & Sangwan, 2021). Workplace gender diversity describes the gender composition of the workforce while gender inclusion refers to the extent to which organisational culture and policies foster a feeling of acceptance amongst female workers (Garg & Sangwan, 2021). Efforts designed to increase gender diversity – such as the implementation of gender targets for instance – might not necessarily foster greater gender inclusion (Miller & Katz, 2002). Garg and Sangwan (2021) suggest that effective gender inclusion initiatives lift the sense of “belongingness” amongst women in an organisation, which has the impact of attracting more women to the organisation, increasing retention among female workers, and consequently promoting greater gender diversity.



Though some progress on workplace gender equity and inclusion has been made over time, gendered challenges within male dominated fields still present an intractable reality for many organisations. Naturally, gender based challenges are likely to be more pronounced in professions and industries that remain male dominated, where cultural norms that embed outdated gender stereotypes have developed over time (Ridgeway, 2011) and which have the effect of reducing women’s sense of belongingness (Cheryan et al., 2017).

Our review of the literature highlights seven key dimensions of how gender disparities persist in cyber security. These barriers include: under-representation of women, the gender pay gap, inflexible work arrangements, discrimination and sexism, gendered stereotypes towards cyber security, a lack of female leaders and role models and masculinised promotion. These barriers are represented in Figure 2.

**Figure 2:** Barriers to gender diversity and inclusion in cyber security



#### 4.1 Under-representation of women

The lack of female representation – that is, having to work in an environment with significantly more men than women – has been identified as both a manifestation and perpetuator of gender inequality. Working predominantly amongst men, younger women report a sense of being underestimated, while those in more advanced stages of their career report a fear of sexual harassment (Giboney et al., 2023). As Kshetri and Chhetri (2022) have demonstrated in their discussion of a Kaspersky Lab survey of school-aged females, 47 percent report that they would like to work in a field with an equal female to male balance. Further, male dominated professions such as cyber security can have the effect of reducing women’s sense of belongingness (Cheryan et al., 2017). Overall, the ubiquity of men within the workplace environment appears to lead to an unpleasant working environment for women.

## 4.2 Gender pay gap

The gender pay gap in cyber security is both a manifestation and perpetuator of gender inequality since it reflects underlying inequities in career progression opportunities, education opportunities, and treatment in the workplace faced by women. The gender pay gap can stem from two sources: pay differences between men and women who work in the same occupation and level of seniority (i.e. rate of pay) and pay differences that arise from the sorting of men and women into different occupations, industries and employment status (i.e. total pay). The sorting of men and women into occupations can emerge for several reasons, including structural disadvantage due to either limited educational opportunities, career interruptions associated with child rearing responsibilities or because women are discouraged from entering or remaining in high paying occupations that offer limited scope for work-life balance, therefore leading to fewer opportunities for career progression (Goldin, 2014).

As documented earlier in this report, the gender pay gap still exists in cyber security and presents a challenge for women as it hinders their professional growth, limits their opportunities for advancement, and perpetuates a cycle of under-representation and inequity within the industry (Foley et al., 2017). The 'ask gap' also contributes to the gender pay gap in STEM related fields; when applying for engineering jobs, women's asking salary was found to be around three percent lower than male applicants (Roussille, 2024).

## 4.3 Job design and inflexible work arrangements

Surveys of IT and STEM professionals in Australia point to gendered barriers around job design and inflexible work arrangements which contribute to challenges in women achieving work-life balance, particularly for those with caring and family responsibilities (Nielsen et al., 2004). A lack of flexible work arrangements is cited as a key reason why Australian women leave careers in STEM and ICT (Foley et al., 2017). Further, a majority of survey respondents believed that promotions and opportunities for career progression in STEM are largely drawn from the pool of full-time workers, while 70 percent of respondents believed that career interruptions associated with maternity/parental leave was detrimental to their careers (Professionals Australia, 2017).

Job design likely contributes to inflexible work arrangements in male dominated professions. This is because it is common for tasks and responsibilities to be designed with little regard for flexibility (Acker, 1990; Withanaarachchi & Vithana, 2022), leading to problems associated with gender diversity and inclusion. Organisations may set themselves up for gender disparities through expectations for work commitments that extend into late night, 24/7 availability and the need to be extremely focused, which create conflicts with the additional workload often placed on women with domestic responsibilities (Aljuaid, 2022; Bagchi-Sen et al., 2010; Foley et al., 2017). For instance, the nature of work and job design in the IT sector – notably rapid technological change and long working hours – undermine the professional identity that female IT professionals have given possible caring and family responsibilities (Nielsen et al., 2004).

Goldin (2014) attributes gender disparities such as the gender pay gap primarily to job design that favours and rewards workers – namely men – who are willing to sacrifice work-life balance. That is, men have a greater means to work longer hours, engage in ‘face time’ and be available 24/7 (Goldin, 2014). Changes in job design that reduce employers’ demand for workplace flexibility can have the effect of reducing gender disparities. Even where flexible work arrangements are available and widely utilised, working from home can limit career advancement opportunities for women as it can make it more difficult to find mentors and sponsors, lead to

questioning of a person's commitment to the organisation, and impact participation in the workplace as people are less likely to speak up and be heard in hybrid meetings (Haas, 2022).

#### **4.4 Workplace cultural problems around discrimination and sexism**

The male dominated cyber security work environment for women represents a challenge in attracting and retaining women in the profession. Social networks and activities which exclude women are common in male dominated professions (Acker, 1990). These “old boy’s networks”, for instance, may inhibit women’s career progression by reducing their awareness of the political landscape of their organisation, and impede their ability to confidently challenge decisions made by leaders within the organisation through the support of their fellow colleagues (Bagchi-Sen et al., 2010).

According to a 2015 survey of IT professionals, masculinised cultures can exacerbate incidents of harassment, bullying, and unconscious bias (Professionals Australia, 2017). Aljuaid (2022) documents that this hostile environment in cyber security, which includes discrimination, can make cyber security work inherently unappealing to females as it undermines their sense of emotional safety at work. Micro-aggressions such as the valuing of male opinions above those of females constitute another important aspect of negative gender-based experiences for women in cyber security (Aljuaid, 2022; Jordan, 2022; Reed et al., 2017).

## 4.5 Gender stereotypes and a lack of awareness of cyber security develop early

Gendered stereotypes and limited understanding of cyber security is evident among school aged girls, which potentially affect subsequent career choices (Lhammer & Hagman, 2021). Early exposure programs to promote awareness of, and accessibility to cyber security, may themselves be

gender biased in their design; a prime example of this is the Hour of Code program, which integrates coding activities into a video game format – potentially invoking the “gamer” stereotype often



viewed as being unappealing towards girls (Del Toro, 2019). These inequalities are an issue, as Hinojosa et al. (2016) show that interest and confidence in STEM at the secondary school level is a strong predictor of success in post-secondary STEM courses. While informal enrichment activities in the form of camps such as GenCyber increase female interest in pursuing cyber security, access or exposure to these activities shows a gender discriminatory pattern, with Raytheon (2017) documenting that 35 percent of females, as opposed to 16 percent of males, stated that no enrichment activities around cyber security were offered to them through school. Raytheon (2017) also establish that more males (40 percent) than females (28 percent) have had exposure to information about cyber security as a career, with twice as many males (two-thirds of participants) as females (one-third) understanding the job requirements for

cyber security professionals. Further, Hansen et al. (2017) demonstrate the presence of stereotypes in children as young as 7-8 years old, with 71 percent of these participants describing computer scientists as male and 90 percent believing that cyber security work is solitary, lending support to the “solitary hacker” stereotype (Kaspersky, 2018).

## 4.6 Lack of female leaders and role models

A lack of female leaders and senior managers in cyber security is another significant manifestation and perpetuator of gender disparity in the cyber security profession (Ahuja, 2002; Withanaarachchi

& Vithana, 2022). In a study of young people conducted by Kaspersky (2018), over 60 percent of female respondents viewed a career in cyber security positively if they had met someone who works as a cyber security professional, but only 11 percent of the entire survey sample had in fact met a female cyber security professional.

The problem of few female role models extends beyond the workplace to the teaching of STEM subjects at school. Stearns et al. (2016) suggest that girls are more likely to major in STEM areas if they have female science/maths teachers in secondary school. González-Pérez et al. (2020) conclude that a lack of role models during these formative educational experiences contributes to a lack of interest and success in STEM subjects, indicating that the desire for female role models is ubiquitous across female age groups and life stages.

The important influence of teachers is echoed again by Bagchi-Sen et al. (2010) who argue that the interest gap in STEM that arises in grades six to eight, growing larger throughout secondary school, may be attributed to a lack of female teachers in maths and science classrooms as well as lower self-efficacy in computer/IT skills overall. At the tertiary level, the lack of female representation in IT faculties presents a barrier for female students in gaining guidance, and procuring mentoring opportunities (Bagchi-Sen et al., 2010).

#### **4.7 Masculinised promotion of cyber security**

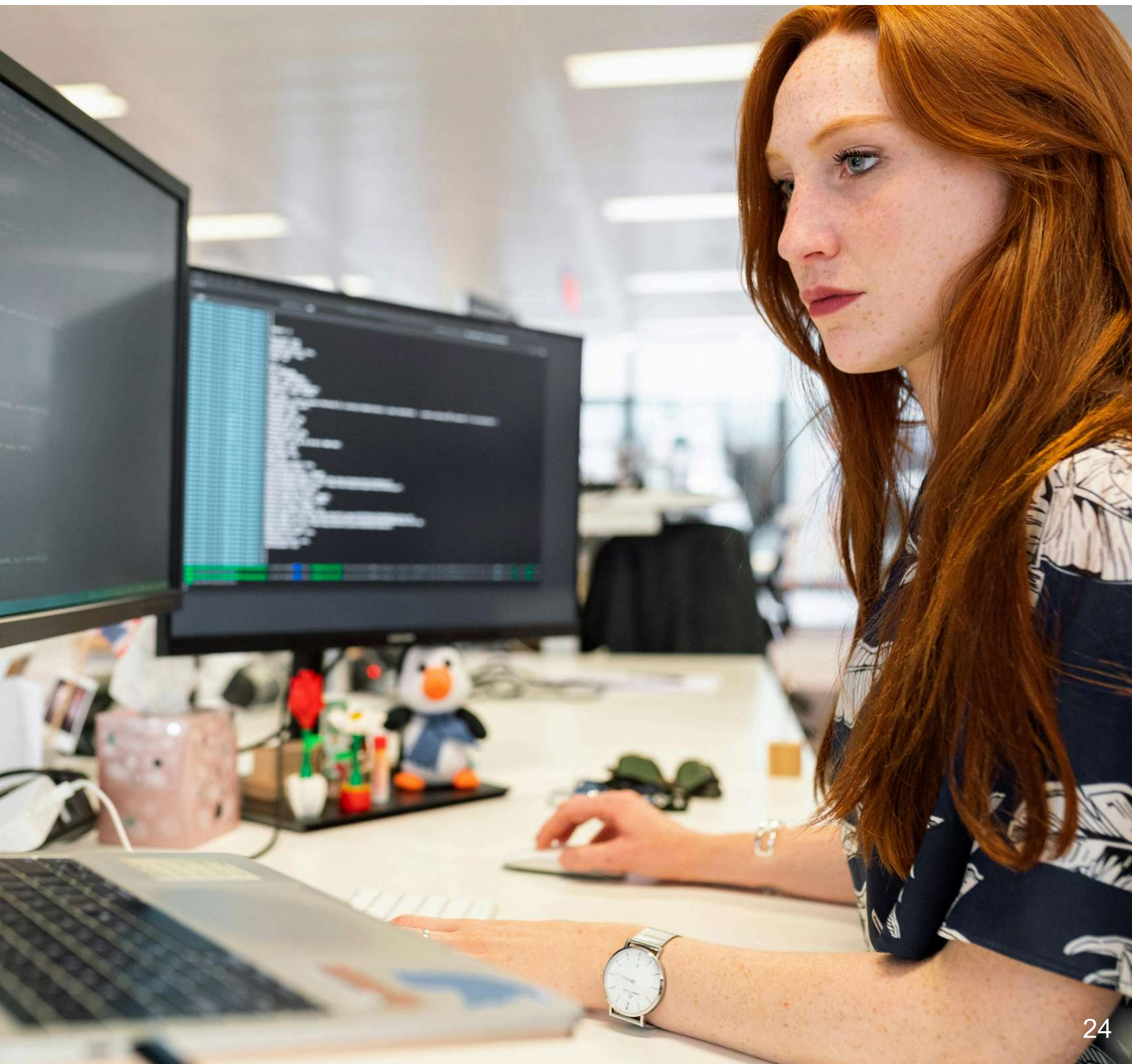
Militaristic analogies about the role of cyber security in protecting the community from cyber attacks and harm promotes the view such roles are a “man’s job” (LeClair & Pheils, 2016; Peacock & Irons, 2017). Compounding this issue further is the “traditional masculinity model of the different roles”, where stereotypes abound that men are perceived as being more naturally fitted to roles of leadership and management while women, on the other hand, struggle to be “productive under pressure” (Aljuaid, 2022, p. 77).

#### **4.8 Summary**

There are myriad factors that contribute to persistent gender disparities in the cyber security workforce. While underrepresentation of women in this sector may be approached with gender inclusion initiatives, this is hindered by enduring issues with the gender pay gap and inflexible work arrangements due to restrictive job design. Added to this, women in the cyber security industry feel subjected to various forms of harassment and micro-aggressions.

Many of these barriers contribute to the perpetuation of gender inequality in part because they can lead to attrition of women from the profession and deter women from considering a career in cyber security. A lack of female leaders in the profession, for instance, leaves key decisions around job design and career progression predominantly up to male leaders which may foster gender equalities.

Enduring gendered stereotypes and societal attitudes can contribute to skill shortages in cyber security because there is a shortfall of women who seek to pursue a career in the field. As such, there is a role for governments and peak bodies to address such external factors. The internal factors considered that pertain to gendered work practices and conditions are within the purview of organisations to change. In the next section, we turn our discussion to initiatives designed to improve gender diversity and inclusion in the cyber security profession.



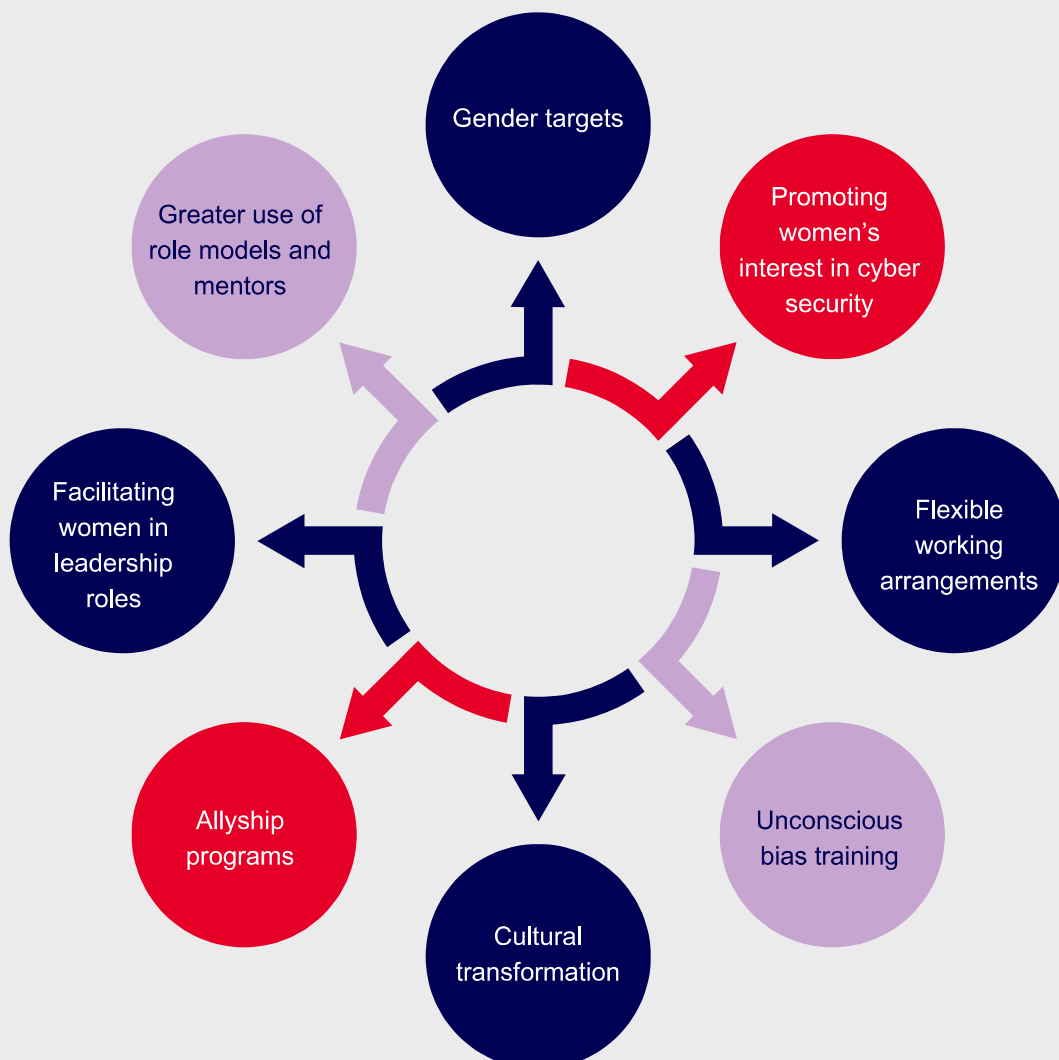


# 5. ENABLERS OF GENDER DIVERSITY AND INCLUSION IN CYBER SECURITY

Women cyber security professionals value their organisation's gender diversity and inclusion culture and policies more than men, and are more likely than men to believe that policies that foster diversity and inclusion are important to overall team performance (ISC2, 2024). There is a growing awareness globally of the need to increase the representation of women and other minority groups in the cyber security workforce to address the growing global shortage of cyber security professionals. For instance, the Diverse Cyber Security Workforce Act proposes to boost diversity in the cyber security workforce in the United States by supporting the recruitment of women and other under-represented groups, including people from disadvantaged communities and older individuals (Rascon, 2024).

Our review of the literature highlights eight key initiatives designed to improve gender diversity and inclusion in cyber security. These enablers include: gender targets, promoting women's interest in cyber security, flexible working arrangements, unconscious bias training, cultural transformation, allyship programs, facilitating women in leadership roles and a greater use of role models and mentors. These enablers are represented in Figure 3.

**Figure 3:** Promoting gender diversity and inclusion in cyber security



## 5.1 Gender targets and disclosure around gender composition

One of the mechanisms in which greater gender diversity in the cyber security profession can lead to better gender inclusion outcomes is addressing the representation of women in cyber security to achieve gender balances (Giboney et al., 2023; Kshetri & Chhetri, 2022). While gender targets do not directly address gender inclusion, greater female representation can place pressure on organisations to improve the workplace culture for women and increase their sense of belonging (Miller & Katz, 2002).

Gender targets however can give rise to a 'competence stigma' among existing employees. In an experimental setting, Leibbrandt et al. (2018) demonstrate that the performance of women selected by a gender target are more likely to be misreported and/or sabotaged than women selected on 'merit'. Additional evidence shows that employees in male dominated professions tend to question the value of skills of women who are seen to be hired to meet organisational gender targets. Ghalebeigi et al. (2022) suggest that organisation-wide mandatory training and education emphasising benefits of gender diversity could help to foster a cultural shift around the implementation of gender targets.



To the extent that gender targets are considered by some to be too heavy handed or risk provoking a backlash, organisations could also consider increasing transparency around gender disparities by disclosing on a regular basis a range of gender equality indicators, including gender representation by levels of seniority and function, gender pay gaps and incidences of harassment and bullying. By increasing the level of disclosure of vertical and horizontal workplace segregation and other gender disparities, organisations may be subject to greater internal and external pressures to improve gender diversity and inclusion.

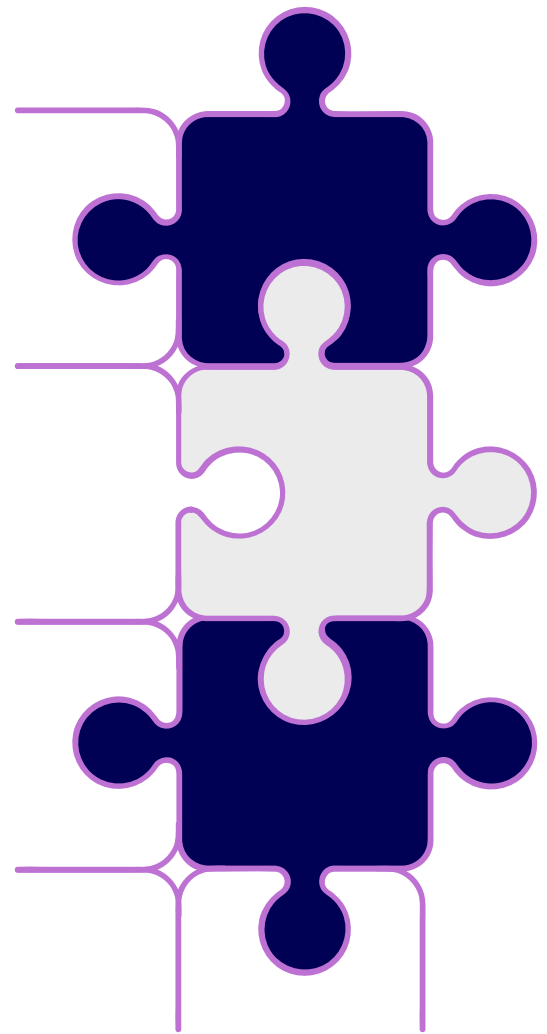
## 5.2 Promoting women's interest in cyber security

Raising awareness about cyber security careers should commence early to have the greatest impact of challenging gendered stereotypes about the profession and nature of work, with the promotion of certain types of skills helping to encourage women's interest in the field of cyber security (OECD, 2023). Jethwani et al. (2017) have shown that an emphasis on creative and collaborative problem-solving, as well as real world application can increase female interest in working in the field (Kshetri & Chhetri, 2022; Withanaarachchi & Vithana, 2022). A focus on "real world and social issues" has also been suggested by some, as well as greater focus on how the field of cyber security can help others (DeCrosta, 2021; Kam et al., 2022).

## 5.3 Flexible work arrangements

The cyber security profession would become more attractive to women as a career choice by expanding the list of attributes and behaviours rewarded. By shifting away from a "hacker culture" that prizes long hours, late nights, and an "obsessive" 24/7 focus, the profession would likely diminish the feeling among women that cyber security work is not suited to them and better accommodate caring responsibilities (Aljuaid, 2022; Bagchi-Sen et al., 2010; Poster, 2018). Considering the significant representation of women in part-time work, equal opportunities offered to both full- and part-time workers could form part of this implementation (Professionals Australia, 2017).

However, researchers have identified the presence of a "flexibility stigma" associated with women (and men) taking advantage of flexible work arrangements in work cultures that value long working hours and an unstinting commitment to work responsibilities (Padavic et al., 2020), which can have adverse consequences for career advancement (Goldin, 2014). It remains to be seen whether the involuntary shift to working from home during the global pandemic for many organisations leads to a permanent shift in favour of more flexible work arrangements and a reduction in the "flexibility stigma". Given the nature of cyber security work which focuses on protecting organisations and individuals from cyber-attacks from increasingly sophisticated cyber criminals (Curtis & Oxburgh, 2023), it may be challenging to persuade senior cyber security leaders that the workday of employees ends when they leave the office for the day.



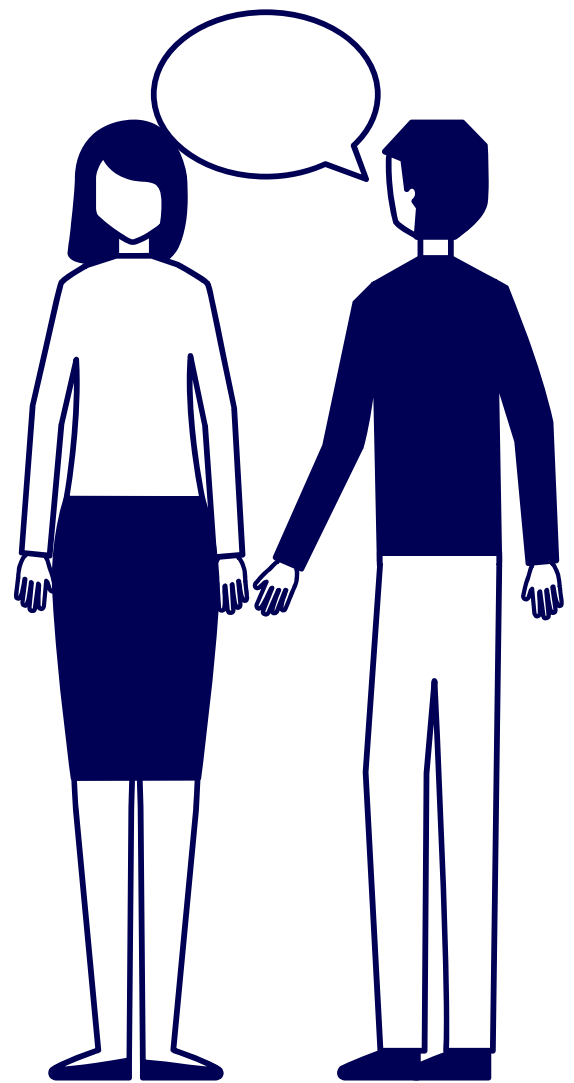


## 5.4 Mandatory unconscious bias training

The research on the efficacy of unconscious bias training is mixed. On the one hand, it has been shown that mandatory unconscious bias training can help to transform masculinised gender norms by confronting the underlying cultural factors contributing to workplace gender inequality (Madsen & Andrade, 2018). Two channels through which such training can be effective at shifting cultural norms are to raise awareness of unconscious or invisible bias that both men and women exhibit, and to challenge conventional views that stereotypically masculine leadership styles are superior to stereotypically feminine styles (Madsen & Andrade, 2018). Andrade (2024) suggests that training and development to address unconscious gender bias in the workplace should emphasise three strategies: safe spaces for women to share experiences, self-reflection on leadership beliefs and styles, and alternatives to gendered and stereotypical leadership styles. On the other hand, in their analysis of policies and practices in the Australian Public Service, Williamson and Foley (2018) draw attention to the possibility that unconscious bias training can have the unintended effect of entrenching and normalising unconscious biases, and recommend that such training be complemented by affirmative action such as setting gender targets to foster women's career advancement.

## 5.5 Cultural transformation

On account of the negative effects of over-masculinised cultures on female recruitment and retention, it has been suggested that it is essential that organisations involved in providing cyber security services demonstrate gender neutrality in their workplace culture (Withanaarachchi & Vithana, 2022). One way this can be achieved is through the use of gender-neutral language (Da Silva & Jensen, 2022). Organisations should consider the effect of masculine cyber security “protector” tropes, such as those of “shadow warriors”, in the promotion of the field may have on women’s sense of interest and belonging in cyber security roles (Da Silva & Jensen, 2022). At the organisational level, progress towards achieving gender inclusion could include the regular provision of Pulse surveys of employee engagement to gauge internal perceptions of gender equality (Fitzsimmons et al., 2020) with scope to link senior managers’ KPIs to making measurable progress on gender diversity and inclusion (Fitzsimmons et al., 2020).



## 5.6 Allyship programs

Allyship programs are initiatives that involve individuals actively supporting and advocating for marginalised or under-represented groups. In the context of cyber security and other male dominated professions more broadly, men would be recruited to advocate for the rights of women in the workplace, including greater gender equity and fostering a culture that promotes opportunities for career progression among women (Bilal et al., 2021; Moser & Branscombe, 2022). In a profession where men occupy the majority of leadership positions, male allies in cyber security are likely to be influential in effecting change that fosters a more inclusive and equitable workplace where everyone feels valued, respected, and empowered to succeed. Allyship initiatives include men advocating for greater organisational change, raising awareness around the gendered barriers faced by women in the organisation and profession, establishing committees and other formal processes and practices that facilitate workplace gender equality, and developing informal networks and mentoring opportunities to support women (Moser & Branscombe, 2022).

## 5.7 Women in leadership roles

A lack of career advancement is a significant motivator for attrition in the cyber security workforce, so offering more promotions would likely increase retention by reducing the sense of stagnation commonly experienced by females working in cyber security (DeCrosta, 2021). Having women in leadership roles may serve to elevate awareness of the challenges women encounter among organisational management, potentially increasing the amount of attention and energy dedicated to creating an environment hospitable to women within the organisation (Aljuaid, 2022). Employers and senior leaders must also be aware of their own unconscious biases, such as the tendency to masculinise leadership roles, as these may form part of the mechanism responsible for women's under-representation in senior management positions (Aljuaid, 2022).

According to Bagchi-Sen et al. (2010), the recognition received by women in the form of appearance on boards or panels, positions within the management team, recognition by executives, and contribution to creation of industry standards, all play a role in defining success for women themselves and may be as equally important as salary in motivating women to participate in cyber security work. This research also suggests that females transitioning from technical to managerial roles may face challenges in being assertive, being able to say no, and marketing themselves and their ideas, which can be addressed via training programs.

Studies in the wider literature beyond the STEM setting have drawn attention to how women only training programs (WOTPs) can facilitate women's career advancement (Chasserio & Bacha, 2024; Chuang, 2019). Benefits that can emerge from WOTPs include fostering improved self-efficacy (Chasserio & Bacha, 2024), deepening women's understanding of their own managerial styles (Chuang, 2019), and helping to clarify attitudes about themselves in their careers and personal lives (Vinnicombe & Singh, 2002).

## 5.8 Female role models and mentoring opportunities for women in cyber security

The presence or the prospect of mentors has been shown to encourage women to pursue a career in cyber security (Jethwani et al., 2017; Withanaarachchi & Vithana, 2022). Further, the lack of mentorship opportunities represents a barrier to career advancement for women in male dominated professions such as cyber security (Bagchi-Sen et al., 2010; Foley et al., 2017). Partnerships between female cyber security professionals across different organisations and industries have been suggested to facilitate mentoring, career advancement and greater job-relevant, practical knowledge (Bagchi-Sen et al., 2010; DeCrosta, 2021). Industry peak bodies such as AWSN can help to facilitate networking programs that transcend organisational boundaries and that are designed specifically for women.





Drury et al. (2011) suggest that female role models in STEM fields can improve recruitment and retention of women by improving women's performance and sense of belonging, while the OECD suggests that role models in industry and policy making can help to challenge gendered stereotypes about the role of women in cyber security (OECD, 2023). Increasing female visibility and creating a community of female workers, complete with role models and mentors, is a crucial aspect of attracting and retaining women in cyber security positions. Facilitating talks and speeches delivered by women, as well as facilitating inclusion of women on boards and panels, may enhance women's sense of achievement and job satisfaction whilst simultaneously increasing the availability of potential mentors and role models for other women (Del Toro, 2019; Kshetri & Chhetri, 2022).

As expressed by participants in the study by Aljuaid (2022), women in cyber security must "talk and give speeches" (p. 75), to educate other women on the workings of the field, and the benefits such a career may offer them. Having "more leadership positions for women" (p. 83) as academics or industry practitioners, is perceived by women as important not only in equalising the gender balance within upper levels of seniority, but also in allowing the female voice to "be heard" (p. 83) and facilitating greater top-down action regarding the challenges faced by women in this field (Aljuaid, 2022).

The visibility of other women, and witnessing their success, is important in motivating and encouraging other girls and women to join and stay in the field (Rowland & Noteboom, 2019). Another important aspect of increasing visibility is the direct impact this would have on female social networks and sense of belonging. Studies have highlighted women expressing a sense of disadvantage due to the prevailing 'boys' club' atmosphere within cyber security, which must be replaced with a sense of female community to foster confidence and enjoyment in work for female workers (Bagchi-Sen et al., 2010; Lingelbach, 2018).

## 5.9 Summary

We have reviewed a range of initiatives drawn from the literature that are designed to reduce gender inequities in cyber security. These include enablers such as the implementation of gender targets or increased disclosure of gender equality indicators, advancing women's interest in the field of cyber security through the promotion of creative and problem-solving skills and a re-framing of job design in cyber security away from a 24/7 culture that values long working hours. Added to this we have also outlined practices that foster a gender inclusive culture and support women's career progression opportunities such as unconscious bias training, the implementation of gender-neutral language and allyship and mentoring programs. In the final section, we conclude our findings and discuss avenues for future research in this area, notably implementation issues associated with the initiatives proposed.





# 6. CONCLUSION



This report has reviewed academic literature on the topic of gender diversity and inclusion in cyber security with a view to understanding the pattern of low female representation in both Australia and internationally and other dimensions of gender disparity. In **Section 2** we demonstrated that studies that focus on gender in Australia's cyber security workforce are sparse, with Bongiovanni and Gale (2023) representing the only study to our knowledge that has examined gendered barriers in cyber security in Australia. In addition to Phase 1 of our study, many of the studies of gender disparities in cyber security in Australia are focused on STEM occupations more broadly, for example, Foley et al. (2017) or are based on patterns in the

United States (for example, Giboney et al. (2023); Givens (2019) and Sturhonda (2019)). The lack of studies that explore gender dimensions within Australia's cyber security workforce suggests that there is scope for further research into the nature of the gendered barriers facing women and initiatives that could most effectively improve gender diversity and inclusion in the cyber security profession.

Phase 1 of our study provides the most up-to-date and comprehensive quantitative study on women in the Australian cyber security workforce. In that study, we recommended that a multi-pronged, collective, and whole-sector approach is needed to create a more gender equitable and inclusive cyber security sector. First of all, leaders and organisations need to actively promote cultural change. Organisations need to review and monitor their policies and practices to break down gender biases, they also need to set clear goals and targets, including embedding them into managers' KPIs, as a way to take concrete actions in improving women's employment and career experiences.

This needs to be supported by industry associations through programs and initiatives that support women in the sector and that enhance the visibility of women role models for the sector. Industry associations play an especially important role as many cyber security professionals are employed in organisations across different industries (e.g., retail, banking) rather than specialist cyber security firms. Hence, the unique challenges experienced by women cyber security professionals in such diverse industries may not be readily aware and well addressed by their employed organisations, and this is a gap that industry associations can fill in providing a strong network and support.

In addition, governments need to ensure their policies support diversity and inclusion and invest in programs that support more women and those from other minority groups to pursue a career in the sector. Educational institutions are also important players as they help to provide a healthy talent pipeline through inclusive program design and purposeful career development for women.

The second stage of Phase II of this project involves a qualitative analysis based on interviews of 30 female cyber security professionals who each have a minimum of over five years' experience in the cyber security workforce. By examining the lived experiences of these women, many of whom are in mid to senior level positions working in a male dominated profession, we aim to garner a better understanding of the extent to which they have faced gendered barriers. We also seek to learn how they have sought to overcome gendered barriers, and whether they have benefited from initiatives implemented by their organisation to foster gender diversity and inclusion. We will also explore what their motivations were for becoming cyber security professionals, whether they have considered leaving the profession, and what aspects of their role they value most. Insights in this regard would enable organisations and the sector as a whole to devise better policies and practices that retain high calibre women cyber professionals.



# REFERENCES

- Acker, J. (1990). Hierarchies, jobs, bodies: A theory of gendered organizations. *Gender & society*, 4(2), 139-158.
- ACS. (2015). The promise of diversity - gender equality in the ICT profession. <https://www.acs.org.au/insightsandpublications/reports-publications/promise-of-diversity.html>
- Ahuja, M. (2002, 03/01). Women in the Information Technology Profession: A Literature Review, Synthesis and Research Agenda. *European Journal of Information Systems*, 11, 20-34. <https://doi.org/10.1057/palgrave/ejis/3000417>
- Aljuaid, A. (2022). Empowering Women in Saudi Arabia to Access Cyber Security Opportunities: A Qualitative Study ProQuest Dissertations Publishing].
- Andrade, M. S. (2024). Addressing unconscious gender bias: strategies for leadership development. *Development and learning in organizations*, 38(1), 31-33. <https://doi.org/10.1108/DLO-02-2023-0055>
- Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). Women in Cyber Security: A Study of Career Advancement. *IT professional*, 12(1), 24-31. <https://doi.org/10.1109/MITP.2010.39>
- Beckhusen, J. (2016). Occupations in Information Technology. *American Community Survey Reports*, ACS-35.
- Bethlehem, J. (2010). Selection bias in web surveys. *International statistical review*, 78(2), 161-188.
- Bilal, M., Balzora, S., Pochapin, M. B., & Oxentenko, A. S. (2021). The Need for Allyship in Achieving Gender Equity in Gastroenterology. *The American journal of gastroenterology*, 116(12), 2321-2323. <https://doi.org/10.14309/ajg.0000000000001508>
- Bongiovanni, I., & Gale, M. (2023). Women in Cyber: Exploring the Barriers, Redesigning the Profession.
- Bureau of Labor Statistics (BLS). (2024). Highlights of women's earnings in 2021. Accessed 24 June 2024. <https://www.bls.gov/opub/reports/womens-earnings/2021/home.htm>. Accessed on 10 June 2024.
- Cech, E. A., & Blair-Loy, M. (2019). The changing career trajectories of new parents in STEM. *Proceedings of the National Academy of Sciences*, 116(10), 4182-4187.
- Chasserio, S., & Bacha, E. (2024). Women-only training programmes as tools for professional development: analysis and outcomes of a transformative learning process. *European Journal of Training and Development*, 48(3/4), 455-477.
- Cheryan, S., Ziegler, S. A., Montoya, A. K., & Jiang, L. (2017). Why are some STEM fields more gender balanced than others? *Psychological bulletin*, 143(1), 1.
- Chuang, S. (2019). Exploring women-only training program for gender equality and women's continuous professional development in the workplace. *Higher Education, Skills and Work-Based Learning*, 9(3), 359-373.
- Cohen, P. N. (2013). The persistence of workplace gender segregation in the US. *Sociology Compass*, 7(11), 889-899.
- Coutinho, S., Bollen, A., Weil, C., Sheerin, C., Silvera, D., Donaldson, S., & Rosborough, J. (2023). Cyber Security Skills in the UK Labour Market

- Crumpler, W., & Lewis, J. A. (2022). Cyber Security Workforce Gap. JSTOR.
- Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal*, 96(4), 573-592. <https://doi.org/10.1177/0032258x221107584>
- Da Silva, J., & Jensen, R. B. (2022). " Cyber security is a dark art": The CISO as Soothsayer. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2), 1-31.
- DeCrosta, J. (2021). Bridging the Gap: An Exploration of the Quantitative and Qualitative Factors Influencing the Cyber Security Workforce Shortage ProQuest Dissertations Publishing].
- Del Toro, E. (2019). Introducing Women to Computer Science in High School to Reduce the Gender Gap in the Cyber Security Profession ProQuest Dissertations Publishing].
- Department of Home Affairs (2023). 2023-2030 Australian Cyber Security Strategy. <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy>
- Department of Industry, Science and Resources (2023). STEM-qualified occupations. Department of Industry, Science and Resources. <https://www.industry.gov.au/publications/stem-equity-monitor/workforce-data/stem-qualified-occupations>
- Drury, B. J., Siy, J. O., & Cheryan, S. (2011). When do female role models benefit women? The importance of differentiating recruitment from retention in STEM. *Psychological Inquiry*, 22(4), 265-269.
- Fitzsimmons, T. W., Yates, M. S., & Callan, V. J. (2020). Employer of Choice for Gender Equality: Leading practices in strategy, policy and implementation. Brisbane: AIBE Centre for Gender Equality in the Workplace.
- Foley, M., Dewey, L., Williamson, S., Blackman, D., Creagh, A., Davidson, L., Zhu, M., & Slay, J. (2017). Women in cyber security literature review.
- Garg, S., & Sangwan, S. (2021). Literature Review on Diversity and Inclusion at Workplace, 2010–2017. *Vision*, 25(1), 12-22. <https://doi.org/10.1177/0972262920959523>
- Ghalebeigi, A., Gekara, V., Douglas, K., Ferraro, S., Wang, L., & Safari, M. (2022). Assessing Progress in Implementing the Gender Equality Act 2020.
- Giboney, J. S., Anderson, B. B., Wright, G. A., Oh, S., Taylor, Q., Warren, M., & Johnson, K. (2023). Barriers to a cyber security career: Analysis across career stage and gender. *Computers & security*, 132, 103316. <https://doi.org/10.1016/j.cose.2023.103316>
- Givens, E. W. (2019). Perception versus Reality: The Perceived Cyber security Workforce Shortage in the United States Capitol Technology University.
- Glass, J. L., Sassler, S., Levitte, Y., & Michelmores, K. M. (2013). What's so special about STEM? A comparison of women's retention in STEM and professional occupations. *Social forces*, 92(2), 723-756.
- Goldin, C. (2014). A grand gender convergence: Its last chapter. *American economic review*, 104(4), 1091-1119.

González-Pérez, S., Mateos de Cabo, R., & Sáinz, M. (2020). Girls in STEM: Is it a female role-model thing? *Frontiers in psychology*, 11, 564148.

Haas, M. (2022). Women face a double disadvantage in the hybrid workplace. *Harvard Business Review*.

Hansen, A., Dwyer, H, Iveland, A, Talesforce, M, Wright, L, Harlow, D, & Franklin D. . (2017). Assessing children's understanding of the work of computer scientists: The draw a-computer-scientist test ACM SIGCSE Technical Symposium on Computer Science Education, Seattle, Washington, United States.

Hinojosa, T., Rapaport, A., Jaciw, A., & Zacamy, J. (2016). Exploring the Foundations of the Future STEM Workforce: K-12 Indicators of Postsecondary STEM Success. REL 2016-122. Regional Educational Laboratory Southwest.

ISC2. (2018). Women in cyber security. [www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx](http://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx)

ISC2. (2023). How the economy, skills gap and artificial intelligence are challenging the global cyber security workforce. <https://www.isc2.org/Research/Economy-Skills-Gap-AI-Cybersecurity-Workforce>

ISC2. (2024). Women in cyber security: Inclusion, advancement and pay equity are keys to attracting and retaining more women.

Jethwani, M. M., Memon, N., Seo, W., & Richer, A. (2017). "I Can Actually Be a Super Sleuth" Promising Practices for Engaging Adolescent Girls in Cyber Security Education. *Journal of Educational Computing Research*, 55(1), 3-25.

Jordan, C. A. (2022). Exploring the Cyber Security Skills Gap: A Qualitative Study of Recruitment and Retention from a Human Resource Management Perspective ProQuest Dissertations Publishing].

Kam, H. J., Ormond, D. K., Menard, P., & Crossler, R. E. (2022). That's interesting: An examination of interest theory and self-determination in organisational cyber security training. *Information systems journal* (Oxford, England), 32(4), 888-926. <https://doi.org/10.1111/isj.12374>

Kaspersky. (2018). Beyond 11%. A study into why women are not entering cyber security. <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.agec.org.au/wp-content/uploads/2018/09/Beyond-11-A-study-into-Why-Women-are-not-Entering-Cybersecurity-2017.pdf>

Kshetri, N., & Chhetri, M. (2022). Gender asymmetry in cyber security: socioeconomic causes and consequences. *Computer*, 55(2), 72-77.

LeClair, J., & Pheils, D. (2016). Women in cyber security. BookBaby.

Leibbrandt, A., Wang, L. C., & Foo, C. (2018). Gender quotas, competitions, and peer review: Experimental evidence on the backlash against women. *Management Science*, 64(8), 3501-3516.

Lihammer, S., & Hagman, L. (2021). Investigating Gender Disparity within Cyber Security: Analysis of Possible Factors Through a Mixed-Method Qualitative Study and a Self-Implemented Testing Program.

Lingelbach, K. K. (2018). Perceptions of Female Cyber Security Professionals toward Factors that Encourage Females to the Cyber Security Field ProQuest Dissertations Publishing].

Madsen, S. R., & Andrade, M. S. (2018). Unconscious Gender Bias: Implications for Women's Leadership Development. *Journal of leadership studies* (Hoboken, N.J.), 12(1), 62-67. <https://doi.org/10.1002/jls.21566>

Miller, F. A., & Katz, J. H. (2002). *Inclusion breakthrough : unleashing the real power of diversity* (1st ed. ed.). Berrett-Koehler Publishers.

Moser, C. E., & Branscombe, N. R. (2022). Male Allies at Work: Gender-Equality Supportive Men Reduce Negative Underrepresentation Effects Among Women. *Social psychological & personality science*, 13(2), 372-381. <https://doi.org/10.1177/19485506211033748>

Mundy, L. (2017). *Code girls: The untold story of the American women code breakers of World War II*. Hachette Books.

Nielsen, S. H., Von Hellens, L., & Beekhuyzen, J. (2004). Challenge or Chaos: A Discourse Analysis of Women's Perceptions of the Culture of Change in the IT Industry. *Issues in informing science & information technology education*, 1, 715-727. <https://doi.org/10.28945/771>

OECD. (2023). *Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom, and United States*. (OECD Skills Studies).

Padavic, I., Ely, R. J., & Reid, E. M. (2020). Explaining the Persistence of Gender Inequality: The Work–family Narrative as a Social Defense against the 24/7 Work Culture. *Administrative Science Quarterly*, 65(1), 61-111. <https://doi.org/10.1177/0001839219832310>

Peacock, D., & Irons, A. (2017). Gender inequality in cyber security: Exploring the gender gap in opportunities and progression. *International Journal of Gender, Science and Technology*, 9(1), 25-44.

Poster, W. R. (2018). Cybersecurity needs women. *Nature* (London), 555(7698), 577-580. <https://doi.org/10.1038/d41586-018-03327-w>

Potter, L. E., & Vickers, G. (2015). What skills do you need to work in cyber security? A look at the Australian market. *Proceedings of the 2015 ACM SIGMIS conference on computers and people research*,

Prieto-Rodriguez, E., Sincock, K., Berretta, R., Todd, J., Johnson, S., Blackmore, K., Wanless, E., Giacomini, A., & Gibson, L. (2022). A study of factors affecting women's lived experiences in STEM. *Humanities and Social Sciences Communications*, 9(1), 1-11.

Professionals Australia (2017). *Women in Engineering: Realising Productivity and Innovation Through Diversity*. Professionals Australia, Melbourne, Australia

Rascon, J. (2024). House Bill Aims for Diverse Cyber Workforce, MeriTalk. Accessed 24 July 2024. <https://www.meritalk.com/articles/house-bills-aims-for-diverse-cyber-security-workforce/>

Raytheon. (2017). *Securing Our Future: Cyber Security and the Millennial Workforce*.

Reed, J., Zhong, Y., Terwoerds, L., & Brocaglia, J. (2017). The 2017 global information security workforce study: Women in cyber security. Frost & Sullivan White Paper.

Ridgeway, C. L. (2011). *Framed by Gender: How Gender Inequality Persists in the Modern World* (1 ed.). Oxford University Press.  
<https://doi.org/10.1093/acprof:oso/9780199755776.001.0001>

Risse, L., Beamond, M., Hall, J., Wang, Y., Warren, M., Barua, B., & Kondylas, L. (2023). *Gender Dimensions of the Australian Cyber security Sector*.

Roussille, N. (2024). The Role of the Ask Gap in Gender Pay Inequality. *The Quarterly Journal of Economics*, 139(3), 1557-1610. <https://doi.org/10.1093/qje/qjae004>

Rowland, P., & Noteboom, C. (2019). *INFLUENCING THE FUTURE: ADOLESCENT GIRLS' PERCEPTIONS OF CYBERSECURITY CAREERS*.

Stearns, E., Bottía, M. C., Davalos, E., Mickelson, R. A., Moller, S., & Valentino, L. (2016). Demographic characteristics of high school math and science teachers and girls' success in STEM. *Social Problems*, 63(1), 87-110.

Sturhonda, J. (2019). *The Underrepresentation of Females in the United States Cyber Security Workforce: A Multiple-case Study* [ProQuest Dissertations Publishing].

Vinnicombe, S., & Singh, V. (2002). Women-only management training: An essential part of women's leadership development. *Journal of Change Management*, 3(4), 294-306.

Williamson, S., & Foley, M. (2018). Unconscious bias training: The 'Silver Bullet' for gender equity? *Australian journal of public administration*, 77(3), 355-359. <https://doi.org/10.1111/1467-8500.12313>

Withanaarachchi, A., & Vithana, N. (2022). Female underrepresentation in the cyber security workforce – a study on cyber security professionals in Sri Lanka. *Information and computer security*, 30(3), 402-421. <https://doi.org/10.1108/ICS-08-2021-0129>