Gender Dimensions of the Australian Cyber Security Sector - Report

Steps to a more inclusive Cyber Security workforce for women in Australia

2023

RMIT UNIVERSITY
Centre for Cyber Security Research and Innovation

awsn
Australian Women in Security Network

Acknowledgement of Country

RMIT University acknowledges the people of the Woiwurrung and Boon wurrung language groups of the eastern Kulin Nations on whose unceded lands we conduct the business of the University. RMIT University respectfully acknowledges their Ancestors and Elders, past and present.

RMIT also acknowledges the Traditional Custodians and their Ancestors of the lands and waters across Australia where we conduct our business.

Artwork: *Luwaytini* by Mark Cleaver, a proud Palawa person and RMIT Master of Human Resource Management student.

Foreword

It is my distinct pleasure to introduce this report, 'Gender Dimensions of the Australian Cyber Security Sector - Opportunities and Challenges'. The RMIT Centre for Cyber Security Research and Innovation (CCSRI) has brought together a multi-disciplinary team of academics to examine this multi-dimensional issue. We are proud to author this report which we hope will help shape the conversation and guide practical steps to build a more inclusive and equitable cyber security workforce in Australia.

While it has been widely remarked that women are under-represented in this sector, there is relatively little data available on the exact number of women in Australia's cyber security workforce, their experiences and the roles they are filling. In the wake of growing global security staff and digital skills shortages, this situation is particularly concerning. The expanding importance of the security sector across the economy, combined with an increasing awareness of the value of diversity and inclusive representation in professional contexts, points towards the need for a dedicated analysis of the gender composition of the cyber security industry in Australia.

This report contributes to addressing this knowledge gap. It examines the gender composition of the Australian cyber security workforce and the types of roles that women in the sector are undertaking by drawing on the results from our survey, Australian Census data and existing literature. Additionally, this report enhances our understanding of the factors that support women's involvement in the cyber security industry as well as the barriers that prevent women from joining, staying and thriving in the field. The insights generated from this study will help shape best practices to attract and retain more women in the cyber security sector and to foster a more equitable workforce culture. This investment will provide organisations, such as the Australian Women in Security Network (AWSN), with accurate baseline data to measure the effectiveness of their intervention programs and track changes in women's participation in and contribution to the industry over time.

Rather than promoting a widespread rhetorical commitment to enhance gender equity in the sector, this report stresses the importance of taking practical actions to create a workforce culture in Australia that is genuinely inclusive and that embraces diversity as a strength – one in which women are respected, supported, and heard.

In this report, the authors identify some of the underlying reasons for women's under-representation in the Australian cyber security industry and identify evidence-based approaches to expand the sector's talent pool to best equip it for the growing challenges and demands it faces. At RMIT University, we are excited and proud to collaborate on this important initiative that supports the diversification and dynamism of the Australian cyber security sector and gender equity at large.

Professor Matt Warren,

Director of the RMIT Centre of Cyber Security Research and Innovation, RMIT University

RMIT Academic Research Team

Dr Leonora Risse

Senior Lecturer in Economics

Dr Leonora Risse is an economist with interest and expertise in gender equality, labour economics, economic psychology, demographic and population economics, education, disadvantage, and wellbeing.

Dr Maria Beamond

Lecturer in Management

Within People in Organisations or HRM (Human Resource Management), Dr Maria Beamond's research interests focus on: international HRM, corporate strategies (global talent management, corporate social responsibility, climate change), shared value, emerging economies, artificial intelligence, knowledge management, and managerial decision-making.

Dr Joanne Hall

Senior Lecturer in Cyber Security

Dr Joanne Hall is interested in the mathematics of cryptography, with a particular interest in quantum key distribution. Her role as Program Manager for the Master of Cyber Security degree has broadened her research interests to include curriculum design, skills and diversity in cyber security and the challenges facing small businesses.

Associate Professor Lena Wang

Co-Director, RMIT Centre for People, Organisation and Work

Ying (Lena) Wang is an Associate Professor at the School of Management and a current Co-Director of Centre for People, Organisation and Work (CPOW). Lena teaches and researches in areas of work psychology and organisational behaviour, with focus on leadership, personality, diversity, and employee wellbeing.

Professor Matt Warren

Director, RMIT Centre for Cyber Security Research & Innovation

Professor Matt Warren is the Director of the RMIT Centre for Cyber Security Research and Innovation and a Professor of Cyber Security at RMIT University, Australia. Professor Warren is a researcher in the areas of cyber security and computer ethics.

Dr Banya Barua

Research Fellow, RMIT Centre for Cyber Security Research & Innovation

Banya has completed doctoral studies in workplace wellbeing. Her research focus is on psychology and behaviour as it applies to leadership, gender, talent management and workplace wellbeing. She has corporate experience in management in the information technology industry and collaborates with partners in the US and Mexico for her leadership research.

Mr Laki Kondylas

Deputy Director, RMIT Centre for Cyber Security Research & Innovation

Laki Kondylas is the Deputy Director of the RMIT Centre for Cyber Security Research and Innovation. Laki has a wealth of experience nationally and internationally and has held executive roles in both State and Federal Governments as well as in academic Institutions.

Contents

Acknowledgements

This research has been produced as a result of the collaboration between the RMIT Centre for Cyber Security Research and Innovation (CCSRI) and the Australian Women in Security Network (AWSN). The AWSN's involvement in the study has been facilitated through sponsorship support by the Australian Signals Directorate (ASD), one of Australia's peak national security agencies.

In addition to the core project team, this report received additional contributions from Lee-ann Phillips and Amarens Breteler. Data analysis support was provided by Mary-Anne Mwendwa. Project coordination support was provided by Gabriela Cincotta.

The RMIT research team thanks Jacqui Loustau and the team at AWSN as well as Amy Roberts and the team at ASD for their support in the development of this report.

This report uses data collected from various sources and all data is used with permission. Data from the Australian Bureau of Statistics (ABS) has been sourced from the Australian Census of Population and Housing, including through a special data request. The authors thank the ABS officers who assisted with this data request.

The RMIT 'Australian Security Industry Workforce – Understanding Gender Dimensions' survey data was collected with permission under RMIT Ethics Approval Code 25246. The authors thank all survey participants for sharing their experiences by completing the survey.

The findings and views presented in this report were produced independently and are those of the authors only. The suggested citation for this report is "Risse, L, Beamond, M, Hall, J, Wang, Y, Warren, MJ, Barua, B and Kondylas, V 2023, *Gender Dimensions of the Australian Cyber Security Sector Report,* RMIT University Centre for Cyber Security Research and Innovation."

Acronyms, abbreviations and terminology

Acronyms and abbreviations

ABS	Australian Bureau of Statistics
ANZSCO	Australian and New Zealand Standard Classification of Occupations
ANZSIC	Australian and New Zealand Standard Industrial Classification
ASD	Australian Signals Directorate
AWSN	Australian Women in Security Network
CCSRI	Centre for Cyber Security Research and Innovation
ICT	Information and Communications Technology
STEM	Science, Technology, Engineering and Mathematics

Definition of cyber security

This report focuses on cyber security. Information security comprises a broad variety of security concerns that overlap with cyber security, though the two are not synonymous. The Australian Cyber Security Centre defines information security and cyber security as:

Information security refers to the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability (ACSCa).

Cyber security refers to the measures used to protect the confidentiality, integrity and availability of systems, devices and the information residing on them (ACSCb).

Information security and information technology security, including cyber security, encompass the security of any piece of information and any technology that is used to store information.

Explanation of terminology

This report acknowledges that a person's sex and gender are two different concepts.

ABS data presented in this report are in relation to sex, not gender. Sex is based upon the person's sex characteristics, such as their chromosomes, hormones and reproductive organs. Gender is a social and cultural concept. It is about social and cultural differences in identity, expression and experience as a man, woman, or non-binary person. This report uses the terms 'women' and 'men' in reference to both sex and gender.

This report acknowledges that individuals may not identify as a woman/female or a man/male. The survey conducted by RMIT University as part of this report included the following options for responses to gender identity: non-binary, gender-fluid and gender diverse. These individuals comprised 3 per cent of total responses.

Explanation of data sources

Labour force data were sourced from the ABS Census of Population and Housing for 2006, 2011, 2016 and 2021. Analysis based on the Census data is therefore reflective of the total Australian population. The Census is collected during the month of August for the respective Census year. Five new cyber security occupations were introduced in 2021 and are only available in the 2021 Census. Prior to the 2021 Census, the cyber security workforce was counted as part of a broader occupational category called ICT Security Specialists.

The 'Australian Security Industry Workforce – Understanding Gender Dimensions' survey was distributed to the security industry. Of the 660 responses received, 77 per cent of respondents (510) were women and men working in the cyber security sector. This report presents the results of the security industry data in its entirety to ensure the rigour and future replicability of the survey results. Analysis shows that including the responses of those from the wider security industry does not skew the survey results, and many of the recommendations are applicable to the broader security industry.

The small number of non-binary, gender-fluid and gender diverse survey responses (3 per cent of total responses) meant there were insufficient responses to be able to draw conclusions about 'non-binary' individuals.

Executive Summary

As cyber security becomes an increasingly critical issue for governments, businesses and everyday citizens in Australia, the number of people in the cyber security workforce is soaring.

Despite the sector's rapid expansion and growing importance, the sector is characterised by a stark under-representation of women. To date, little research in Australia has been undertaken into the exact proportion of women employed in the sector, what roles they are undertaking, and the reasons behind the sector's unbalanced gender composition.

The low level of participation of women in the sector means that the sector is not operating at its full potential. The benefits that diverse workforces bring – through a wider spectrum of skillsets, viewpoints and lived experiences, a deeper capacity for innovation, analysis and problem-solving, and a richer understanding of people and human behaviours – is an opportunity that the sector is well-poised to take advantage of.

The solutions to achieving gender equity are not clear-cut. Increasing women's participation in the sector involves more than simply 'encouraging girls to study IT'. Gender gaps in workforce outcomes can be interpreted as signals of biases and barriers. This means that achieving gender equity is not just about striving to attract more women and under-represented cohorts into the sector; it's about understanding the factors that deter them from joining or cause them to leave the sector. It's about the sector committing to fostering a workforce culture that is genuinely inclusive and that embraces diversity as a strength and equity as a value.

This report gives the Australian cyber security sector a clearer picture of women's representation and an understanding of the factors that enable and impede their career participation and advancement. Its recommendations for action point towards the importance of de-biasing work cultures and adopting evidence-based approaches to enhance inclusivity and diversity in the sector's broad systems and culture.

Making change is not easy. Understanding resistance to change, and the reasons why there might be resistance to gender equity initiatives is a part of the sector's challenge. This report provides the sector with insights to help navigate these hurdles.

A starting point to achieving gender equity is a preparedness to learn and a readiness to do things differently. If Australia's cyber security sector can foster a genuine willingness to change and invest in an authentic appreciation of the gains that can be achieved through greater gender equity, diversity and inclusion, it will be well on its way to creating a more dynamic, vibrant and high-performing sector.

1 Key findings and recommendations

1.1 Key findings: What can the cyber security sector learn from this research?

The key findings of this report provide an informative picture of the workforce:

The under-representation of women in the cyber security sector in Australia indicates that the sector is not reaching its full potential. While skills shortages have intensified the need to attract more women into the sector, the unbalanced gender composition of the sector's workforce is also a sign of gender inequities, biases and barriers. These inequities need to be addressed if the sector is to operate at its best and become truly inclusive and embrace diversity.

Women's share of the cyber security workforce in Australia is small. Women comprised around 17 per cent of cyber security occupations in 2021, compared to men's share of 83 per cent.

- As a newly classified occupation, the 2021 Census is the first time that data on cyber security occupations has been collected in Australia's Census.
- To track changes in women's share of the cyber security sector over time, we can look at the gender composition of ICT Security Specialists which is an occupation classification that includes cyber security occupations. Women comprised around 16 per cent of the ICT Security Specialist category in 2021, a fall from their 19 per cent share in 2006.
- Although women are still in the minority, it is promising that, in the past five years, the number of women in ICT Security Specialist roles has grown slightly faster than the number of men. From 2016 to 2021, women's numbers in ICT Security Specialist roles grew fourfold while men's grew threefold.

Women in the cyber security workforce bring a wider spectrum of **educational backgrounds** to the sector than their male colleagues.

- While two-thirds of male cyber security professionals have educational qualifications in information technology, only around half of females hold qualifications in this field. More women come into the sector with qualifications in business and management, humanities, and creative arts.

There were **different motivating** factors for women and men when choosing to join the security sector.

- Women in the cyber security sector are strongly motivated by the quest to make a difference to society. This was the factor most commonly cited as "strongly influential" in women's decisions to join the security sector, cited by 52 per cent of women, compared to only 44 per cent of men participating in the survey.
- Parents are a more influential factor for women (36 per cent) than for men (28 per cent) when choosing a field of study, while friends are a more influential factor for men (22 per cent) than for women (14 per cent).
- Having the opportunity to fully utilise one's skills is a more common motivating factor for men (44 per cent) than women (35 per cent).

Role models and mentors matter for both men and women. Exposure to both role models and mentors has an impact on all genders, during their training and studies as well as during employment.

On-the-job learning, informal networks and mentoring are perceived by workers of all genders as the most useful **activities that aid career advancement**.

Family and care responsibilities have a disproportionate impact on women's career continuity compared to men working in the sector. Women are more likely than men to have had career breaks, and they generally have longer career breaks due to having children and caring for family members.

The cyber security sector is uniquely **poised to be able to make greater progress on gender equity** than other male-dominated fields.

- The cyber security sector is inherently adaptive, iterative, forward-looking and innovative in nature. These characteristics mean the sector is more likely to be willing to evolve and is less constrained by traditions and conventions which have been shown to be key traits that make a difference in achieving progress on gender equity.
- There is a growing body of research that shows that gender-diverse management teams in the technology sector can positively impact business performance. As a rapidly growing area, the cyber security sector has a promising opportunity to take intentional action now to shape its culture to be one that is gender equitable, inclusive and embracing of diversity, and to capitalise on the business benefits of making this shift.
- It is promising to see strong agreement from all genders participating in the survey that providing additional support to women to advance their careers is perceived as **beneficial for the industry** overall.

There is an opportunity to conduct further research into the experiences of **non-binary individuals** working in the security industry to better understand their specific career aspirations and challenges, and identify factors that would enable a more diverse and inclusive workforce.

1.2 Key recommendations: What action steps can be taken?

A whole-of-sector approach is needed to expand the capacity of the cyber security workforce and achieve a more gender equitable and inclusive sector. All dimensions of society – employers, organisational leaders, government, educational bodies, the media, and the wider community – have a role to play in making changes in their policies, practices and attitudes in relation to gender inequity.

Recommended actions for greater gender equality in the cyber security sector need to be grounded in evidence-based approaches. A growing wealth of research points towards the need to change systems, cultures and conventions, rather than put the onus on individual women to "fit in" to a biased system.

Table 1 identifies a number of practical actions that can be taken by key stakeholder groups to assist in progressing gender equity and inclusion in the Australian cyber security sector.

Table 1: Recommended actions to progress gender equity and inclusion in the cyber security sector

For organisations	■ Implement gender equity, diversity and inclusion policies and programs that target workforce culture and organisational practices rather than attempting to "fix" women. ■ Set clear goals and targets for gender equity in the organisation. Consult with women and other under-represented cohorts within the organisation to articulate goals that could deliver meaningful change. ■ Eliminate toxic work cultures and adopt a positive duty of care to all employees, including a zero-tolerance policy towards sexual harassment. ■ Develop and maintain safe work spaces that respectfully accommodate all genders. ■ Conduct an internal gender pay gap audit to ensure equitable salary and benefits. ■ Use recruiting and promotion practices to address implicit biases in existing systems, such as using a language decoder to remove gendered language in job advertisements. ■ Recognise the skill transferability of workers joining from other sectors and support reskilling and upskilling. ■ Commit to flexible work arrangements, including ensuring that women's credentials and capabilities are not valued less when they return from career breaks. ■ Formalise role model and mentorship programs, including role modelling inclusive behaviour and work-family balance among men. ■ Ensure equal access at all levels to opportunities, including professional development, networking and sponsorship. ■ Collect and analyse data on gender equity, diversity and inclusion and evaluate initiatives to determine effectiveness. ■ Apply an intersectional gender lens to rectify biases and barriers in the workplace impeding women from non-majority cultural, socioeconomic and linguistic backgrounds, different spectrums of ability, and First Nations people, and ensure their strengths and capabilities are fully recognised and valued.

For leaders of organisations	■ Role model a willingness to learn, engage in self-reflection, change behaviours and show vulnerability as part of a journey of personal growth and professional development. ■ Personally promote cultural change that removes gender bias within existing systems. ■ Include gender equity outcomes in executives' and managers' KPIs. ■ Demonstrate commitment to a zero-tolerance approach to sexual harassment. ■ Role model inclusive, respectful and equitable behaviour. ■ Invest in leadership programs that elevate diversity and expand beyond traditional models of leadership.
For governments	■ Implement policies and initiatives that pursue gender equity, diversity and inclusion through cultural and institutional level change, rather than attempting to "fix" women. ■ Apply gender equity conditions to procurement policies, grants and funding, and other forms of industry collaboration. ■ Provide funding and resources for initiatives that promote gender equity in the workforce and include provisions for robust evaluation and sharing of learnings. ■ Support initiatives that encourage women to pursue careers in cyber security.
For professional industry associations	■ Create and implement programs and initiatives that are informed by research evidence and women's lived experiences, including leadership programs that expand beyond conventional models of leadership. ■ Invest in initiatives that lift the visibility and voices of women in the sector. ■ Ensure equal gender representation on boards and committees. ■ Commit to gender balance and diversity of speakers on panels and conferences, and call out instances in the sector where this is not achieved. ■ Create a gender stream in national cyber security conferences that is prioritised in the program. ■ Advocate for evidence-based initiatives to achieve gender equity in workplaces. ■ Explore options for knowledge sharing between organisations. ■ Establish a framework of gender equity measures that organisations can adopt. ■ Collaborate with educational institutions to design and provide initiatives that encourage women to pursue careers in cyber security. ■ Establish a 'women in cyber security' speakers register of women who are available to speak to the media and at other public conference events. ■ Collaborate with media professionals to invest in public speaking and media training opportunities for women in cyber security. ■ Ensure women's contributions are recognised and celebrated in professional awards.
For educational institutions	■ Ensure curriculums are gender inclusive and representative. ■ Analyse educational content for gender bias and stereotypes. ■ Collaborate with industry associations to design and provide initiatives that encourage women to pursue careers in cyber security. ■ Promote inclusive attitudes and behaviours – that is, females are equally as capable in STEM subjects as males – among all students at all ages. ■ Create networking opportunities to improve awareness and support for students and families, including for students who are first-in-family to attend university and participate in post-school education. ■ Ensure female representation and respect at all levels of the institution. ■ Ensure gender inclusiveness and diversity of industry guest speakers. ■ Recognise and highlight women's research and industry achievements and contributions.

For the wider community	■ In media, advertising and popular culture, call out gender stereotypical images and terminology of the sector and replace them with more diverse and equitable representations. ■ Design support systems and networking opportunities that promote gender equity, diversity and inclusion in cyber security. ■ Apply an intersectional gender lens to rectify biases and barriers in the community impeding women from non-majority cultural, socioeconomic, and linguistic backgrounds, different spectrums of ability, and First Nations people, and ensure their strengths and capabilities are fully recognised and valued.
For media and conference organisers	■ Commit to gender balance and diversity of speakers on conference panels and event programs, including keynote speakers. ■ Commit to a gender balanced composition in organising committees. ■ Commit to gender balanced participation and representation in the media in terms of expert commentary, author contributions, and journalists specialising in cyber security topics. ■ In popular culture and advertising, commit to inclusive and diverse representation reflecting the composition and values of the wider community. ■ Collaborate with professional industry associations to create a women's speakers register. ■ Set clear guidelines for respectful interactions across online forums, including allocating resourcing for monitoring online behaviour and enforcing repercussions for violations of guidelines and gender-based online abuse. ■ Apply an intersectional gender lens to rectify biases and barriers in the community impeding women from non-majority cultural, socioeconomic, and linguistic backgrounds, different spectrums of ability, and First Nations people, and ensure their strengths and capabilities are fully recognised and valued.

2 Why is this study needed?

There have been varying studies over the years in Australia which suggest that women's share of the cyber security workforce floats between around 11 to 25 per cent. To date, there has been no comprehensive analysis that accurately describes the types of roles that women are working in within the sector and computes the gender composition of the sector specifically for Australia. To ensure the AWSN is making an impact on attracting, retaining and supporting women to thrive in the cyber security sector, an accurate measurement of baseline data is required. This will enable the AWSN to measure the success of its programs and expand in maturity and influence as a representative professional organisation in Australia's security industry.

This study provides the first independent survey and comprehensive analysis of Census data specifically focussed on the cyber security workforce in Australia. It provides baseline data that will allow for ongoing research and build an understanding of the Australian cyber security sector over time. Monitoring changes in the gender composition of the sector over time will assist in identifying impactful programs and 'what works' to enhance female representation and improve gender equity in the sector.

The findings and recommendations of this study are designed to help inform industry, organisations, and governments in their policy design, as well as help equip the AWSN to achieve its mission to lift the representation of women in Australia's security profession.

2.1 Australia's cyber security sector is rapidly growing

Cyber security is becoming an increasingly critical component in the operation of governments and most businesses. Cyber security specialists can be found in most organisations and are responsible for preserving the confidentiality and availability of information, as well as non-information-based assets that are vulnerable to threats arising from the use of information technology. Indicative of the growth of the sector, cyber security is recognised by the ABS as both a "trending skill" (skills that have become more important over the past five years) and an "emerging skill" (skills that have become more prominent in occupations where they were previously not significant).

Evolution towards a knowledge-based economy means that data and information have become key inputs into business and government operations. This has heightened the cognitive complexity of the skills required in the cyber security sector.

Most ICT occupations, including cyber security, require technical skills in Science, Technology, Engineering and Mathematics (STEM). However, the cyber security sector requires a broader suite of skills and capabilities beyond the technical competencies of STEM. Specialist skills in governance, management and coordination are needed to address systems-level challenges and meet the industry's large-scale cyber security needs.

Understanding sources of cyber threats entails "getting inside the minds" of perpetrators to understand their motives and engaging widely with everyday people to understand their experiences of risk and threats. Cyber security therefore, entails understanding people and motivations for human behaviour. Skillsets in psychology, strategic problem-solving, creativity and innovation also form part of the increasingly sophisticated skillsets required in the sector.

A growing body of research points towards the benefits of diversity for improved decision-making and business outcomes (Dobbin and Kalev, 2022). It is this human element of cyber security that emphasises the importance of cultivating diversity and inclusion within the sector's workforce. The greater the diversity of the workforce's composition, the more effectively the sector will be able to understand human behaviour, pre-empt and manage threats, and respond to the broad and diverse needs of industry and society (Hewlett, Marshall and Sherbin 2013; Rock and Grant 2016; Turban, Wu and Zhang 2019).

2.2 Women's under-representation in cyber security is a sign of gender inequity

While the need for more workers to meet future skills needs is one motivation to investigate women's under-representation in the cyber security sector, women's under-representation in the sector is also problematic in itself.

Most of the fields of study that feed into the cyber security sector, and the workplace cultures of the organisations where many cyber professionals are employed, are male-dominated spheres. This includes the male-dominated fields of study in STEM, such as computer science.

The low level of participation in the sector by women is a sign of the influence of gender biases, stereotypes and inequities that prevail across the sector. In part, these biases reflect inequities in wider society, but there are also some distinctive features of the cyber security sector that replicate and exacerbate these gender-patterned biases and the marginalisation of women.

For example, the stereotypical images of a computer scientist within the media and popular culture is that of a man (Cheryan et al., 2013; Master et al., 2016; Cheryan, Master and Meltzoff, 2022). The “hacker culture” that prevails in the IT world leads to a male-oriented work culture of exceptionally long hours and late nights, which raises concerns about the safety of women working in computer laboratories alone or outside of regular working hours (Bagchi-Sen et al., 2010).

Gender bias in male-dominated fields can encompass behaviours that might seem insignificant, such as demeaning comments or jokes about women not being suited to STEM careers, but these actions convey the message that women do not belong in the field. Furthermore, these actions have implications for women’s safety, dignity and respect because they contribute to fostering a culture of tolerance for gender discrimination and sexual harassment against women in the field. High rates of sexual harassment have been clearly documented in Australia’s STEM sector (Science and Technology Australia, 2019).

Examples of evidence of gender bias include:

- Female students perform worse than male students in maths classes when the teacher holds gender stereotypical beliefs about students’ capabilities (Carlana, 2019).
- Managers in STEM are likely to evaluate a CV with a male name more highly than an equivalent CV with a female name (Begeny, Ryan, Moss-Racusin and Ravetz, 2020).
- When presented with research evidence of the existence of gender bias within the STEM fields, men judged the quality of this research as "less meritorious" than women did (Handley et al., 2015).
- Women in STEM fields experience lower job satisfaction and lower average pay rates than men in STEM fields, as well as when compared to men and women in non-STEM fields (Dockery and Bawa, 2019).
- Opportunities for men to advance their careers more readily than women in male-concentrated fields are accelerated by informal social networks that develop between male managers and male employees (Sobieraj 2018; Cullen and Perez-Truglia 2022).
- Within the broader workforce, women are equally as likely as men to ask for a promotion or pay raise in their current job, but are less likely than men to be successful in their request (Artz, Goodall and Oswald, 2018). Women’s confidence and ambition in the workplace is also not valued and rewarded in the same way as men’s (Risse, 2020).

The impact of these gender biases contributes to the ongoing marginalisation and under-representation of women in traditionally male fields, such as STEM, and works to maintain "masculinised" workforce cultures that sideline women by default (Buengeler, Leroy and De Stobbeleir, 2018; Klambauer et al., 2017). Women’s under-representation in the cyber security sector has been linked to the prevalence of masculinised stereotypes and norms (Department of the Prime Minister and Cabinet et al., 2017).

The existence of gender biases, as evidenced above, means that higher hurdles exist for women to join and advance in male-dominated fields. The male-dominated environment of these workforce cultures can also impede the capacity for women themselves to bring about any change. For example, women can feel deterred from reporting sexual harassment due to the perceived risk of career repercussions (National Academies of Sciences, Engineering and Medicine et al., 2018).

While approaches to correcting women’s under-representation in male-dominated fields commonly focus on trying to encourage more women to enter the field as a matter of individual choice, these examples of gender bias point towards the need to focus instead on the wider cultural norms, institutional policies and social conventions that perpetuate these gender-patterned biases and barriers at a systemic level (Gergis and Kachala, 2021). Similarly, attempting to improve gender equity by changing the individual behaviour of men, such as through diversity training, is not guaranteed to be effective. It is an ambitious task to attempt to simply rely on unconscious bias training to undo individuals’ ingrained behaviours and attitudes: the research evidence points towards the need to de-bias workforce policies, practices and cultures and to focus on breaking down the constrictive societal norms that generate these inequities in the first place (Dobbin and Kalev, 2022).

A key message from the existing research is that it is not the fault of individuals that stereotypes and biases exist. Gender inequities in the workforce are the result of gender norms that perpetuate the status quo and traditional attitudes about men’s and women’s roles in society. Often, these norms are replicated unintentionally by unconscious bias and default responses in our everyday actions, beliefs and thoughts. Building awareness about the impacts of gender norms and understanding how gender norms can constrain the well-being of individuals of all genders is part of the roadmap towards building a more inclusive sector.

These gender inequities suggest that the sector is not currently operating at its peak capacity. A growing body of research shows that a more diverse workforce is more innovative, productive and creative (Lee and Kim, 2020; Miller and Del Carmen Triana, 2009; Post and Byron, 2015; Richard, 2000). Beyond these improved performance outcomes, the sector’s quest for a more equitable and inclusive workforce is also a matter of moral principle and a responsibility that is grounded in human rights.

2.3 Existing measurements of gender composition of the cyber security sector are unclear

Members of the industry have indicated that there is no comprehensive data that reliably measures the gender representation of the Australian cyber security workforce or that describes the types of roles that women in the sector undertake. This has led to uncertainty about the gender composition of the sector: previous estimates of the percentage of women working in cyber security vary between 11 per cent (Frost & Sullivan, 2017; Williamson et al., 2017) and 24 per cent (ISC^2, 2018) globally.

More recently, in its 'Australia's Cyber Security Sector Competitiveness Plan 2020', AustCyber computed that females made up 26 per cent of the Australian cyber security workforce in 2022. The workforce data used to determine this figure were sourced from the aucyberexplorer.com.au website (AustCyber, 2022). According to the Australian Computer Society's 2022 Digital Pulse report (ACS, 2022), the percentage of women working in the wider ICT sector in Australia is at 31 per cent. This is a slight uptick from their 2019 study which computed females' share at 28 per cent (ACS, 2019).

To provide an updated measurement, this study draws on multiple data sources, including a tailored survey of workers in the sector and newly-released Census data made available by the Australian Bureau of Statistics, combined with available research and literature. This study provides answers to a set of questions that are of direct relevance to the sector (Figure 1). The outputs of this study will help guide the sector towards taking action to create a more gender-balanced and diverse workforce in the future.

Figure 1: Key questions of RMIT study

Key questions this study investigates

- What is the number and proportion of women in the cyber security sector in Australia?
- What types of roles in the sector are women undertaking?
- What factors explain women's low involvement in the sector?
- What are the enablers and barriers to women's participation in the sector?
- How can the sector expand its talent pool and create a talent management system that enables women's equal representation, participation and recognition at all levels of the sector?
- What cultural and systems-wide changes need to be made to equip the sector to expand diversity and inclusion more broadly, and to sustain these cultural changes in the future?

(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions Survey.)

3 How was this analysis undertaken?

This report approaches the challenge of improving gender equity in the cyber security sector from the perspective of workers themselves. Using official ABS labour force data, the composition of the sector is profiled at the level of the individual worker. This is complemented by insights from a tailored survey by RMIT, titled 'The Australian Security Industry Workforce – Understanding Gender Dimensions', that explores the motivations that attract people to join the cyber security sector, the challenges and barriers that can discourage them from joining and staying in the sector, the factors that foster career opportunities and advancement, and their perceptions in relation to equity and diversity within the sector.

3.1 ABS data

Official ABS labour market data was collected as part of the Australian Census of Population and Housing and made available through the ABS TableBuilder platform. Occupations that relate to the information security sector were identified using the Australian and New Zealand Standard Classification of Occupations (ANZSCO), which is the official category of occupations used by the ABS (ABS, 2022). In the 2021 Census, cyber security occupations were introduced.

The workforce profile for the study was calculated using the cyber security occupation classifications that were newly introduced in the 2021 Census. Because these cyber occupations were only introduced in the most recent Census, this report's analysis of changes over time were based on the occupational category ICT Security Specialists which are available over multiple Census collections and include cyber-related occupations. These occupations are described

ICT occupation classifications

Information, Communications and Technology (ICT) security occupations (available in Census over time) include:

- **ICT Security Specialists** – Tasks include planning, developing, maintaining, managing and administering organisations' database management systems, operating systems and security policies and procedures to ensure optimal database and system integrity, security, backup, reliability and performance. This involves managing and administering an organisation's ICT security policy and procedures to ensure preventive and recovery strategies are in place and minimising the risk of internal and external security threats.

Cyber security occupation classifications

Cyber security occupations (newly introduced in the 2021 Census) include:

1. **Cyber Governance Risk and Compliance Specialist** – Tasks include leading the governance, risk and compliance for cyber security.
2. **Cyber Security Advice and Assessment Specialist** – Tasks include conducting risk and security control assessments, interpreting security policy and contributing to the development of standards and guidelines, reviewing information system designs, providing guidance on security strategies to manage identified risks, providing specialist advice, explaining systems security and the corresponding strengths and weaknesses. Alternative titles include Cyber Security Adviser; Cyber Security Consultant; ICT Security Adviser; ICT Security Consultant.
3. **Cyber Security Analyst –** Tasks include analysing and assessing vulnerabilities in infrastructure (software, hardware, networks), investigating available tools and countermeasures to remedy detected vulnerabilities, and recommend solutions and best practices. Analysing and assessing damage to the data/infrastructure as a result of security incidents, examining available recovery tools and processes, and recommending solutions. Alternative titles include ICT Security Analyst; Information Security Analyst. Specialisations include Cyber Security Researcher or Vulnerability Researcher; Cyber Security Vulnerability Assessor; Cyber Threat Analyst; Malware Analyst.
4. **Cyber Security Architect –** Tasks include designing a security system or major components of a security system and may head up a security design team building a new security system. Alternative titles include Enterprise Security Architect; ICT Security Architect.

5. **Cyber Security Operations Coordinator –** Tasks include leading the coordination and response to complex cyber security incidents and hunt investigations, managing tasks across teams for incident response and hunt operations, advising leadership on current operational collaborations and contribute to strategic planning, facilitating incident response engagements, assess technical information to develop key messaging. Alternative titles include Cyber Security Operations Manager; ICT Security Administrator. Specialisation: Cyber Security Incident Responder.

Labour force data were sourced from the ABS *Census of Population and Housing* for 2006, 2011, 2016 and 2021. Analysis based on the Census data is therefore reflective of the total Australian population. The Census is collected during the month of August for the respective Census year. The five new cyber security occupations were introduced in 2021 and are only available in the 2021 Census[1]. Disaggregated Census data presented in the report, when expressed as a percentage, may not add up to exactly 100 per cent due to small cell counts and rounding.

3.2 Australian Security Industry Workforce – Understanding Gender Dimensions Survey

To supplement ABS labour force data, RMIT undertook its own survey of workers currently employed in the security industry. Respondents were recruited through the professional networks of the CCSRI and AWSN. Survey responses were collected via an online platform throughout September 2022. The final sample generated 660 complete respondents who were mainly from the cyber security sector. The survey encompasses questions on current job, education and training; career inspiration; role models and mentors; perceptions of the industry and demographic

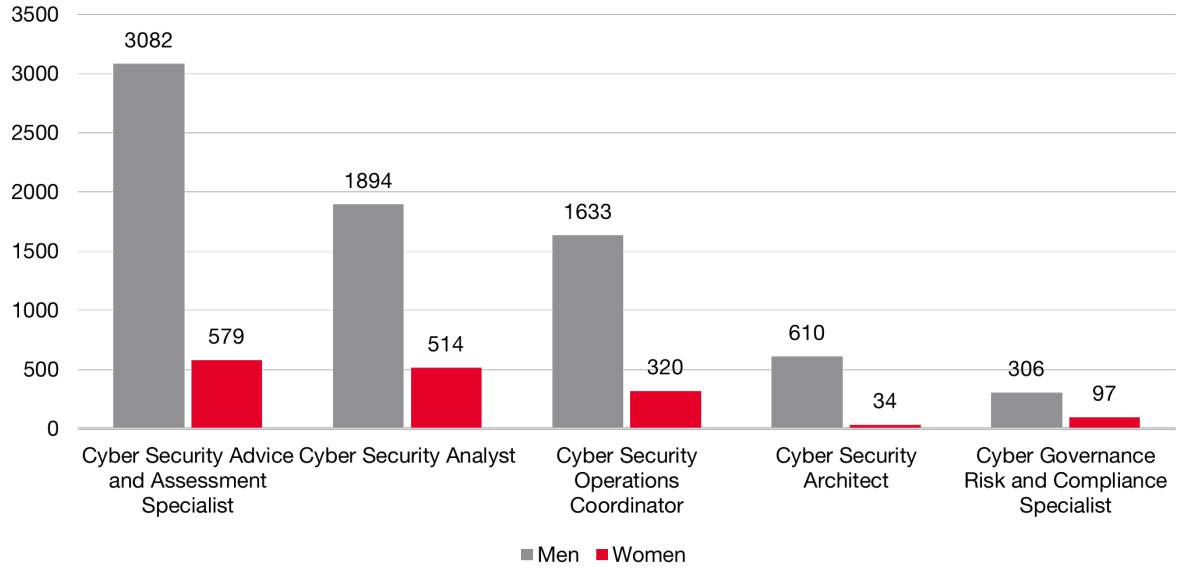
[1] The new cyber occupations supersede some of the job tasks that were previously defined under the ICT Security Specialist occupation, meaning that in some instances the new cyber occupations can be interpreted as a "new title" for the ICT Security Specialist roles. However, some of the new cyber occupations also involve job tasks that were outside of the ICT Security Specialists role, such as tasks relating to governance risk and compliance, which means that they are not directly comparable to the previous ICT Security Specialist roles.

4 What does Australia's cyber security workforce look like?

This report defines cyber security professionals according to the five detailed occupational categories defined by the ABS (Cyber Governance Risk and Compliance Specialist; Cyber Security Advice and Assessment Specialist; Cyber Security Analyst; Cyber Security Architect and Cyber Security Operations Coordinator). Our measurement of the size and profile of the cyber security workforce is based on the sum of the five occupational categories.

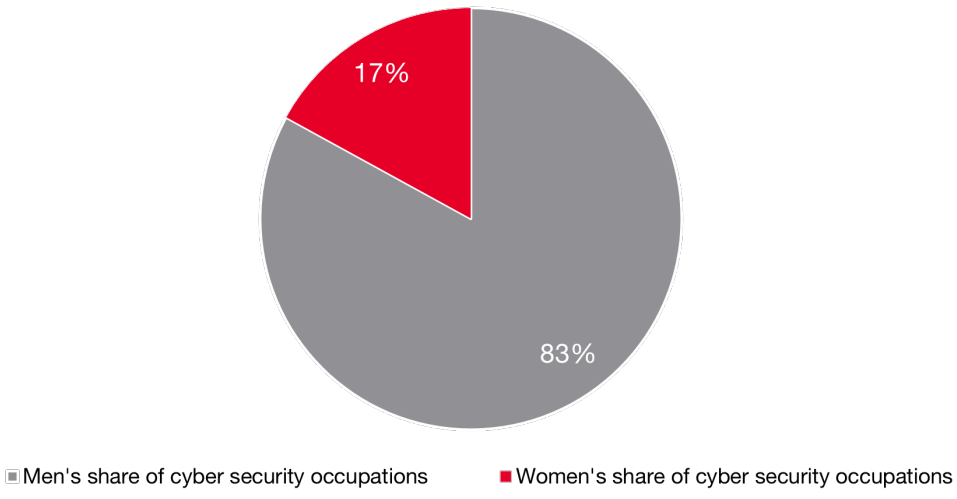
The 2021 Census data shows there are a total of 9,061 people working in cyber security occupations in Australia. Most of these cyber security professionals are in the role of Cyber Security Advice and Assessment Specialist (Figure 2).

Figure 2: Number of cyber security professionals, Australia, 2021



(Source: ABS, Census of Population and Housing, Table Builder, 2021. Cyber occupations were newly introduced for the 2021 Census and therefore only available for this year.)

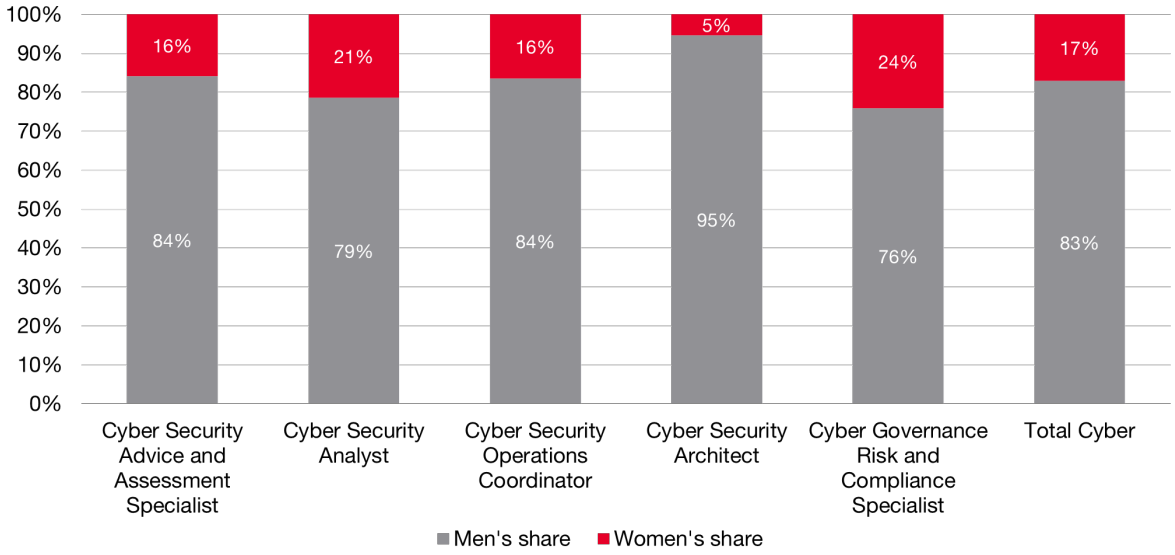
Figure 3: Percentage of cyber security professionals by gender, Australia, 2021



(Source: ABS, Census of Population and Housing, Table Builder, 2021.)

Women comprise 17 per cent of all cyber security professionals (Figure 3). They are mostly employed as Cyber Security Analysts (21 per cent) and Cyber Governance Risk and Compliance Specialists (24 per cent). By contrast, women make up only 5 per cent of Cyber Security Architects (Figure 4).

Figure 4: Gender composition of cyber security professionals, Australia, 2021



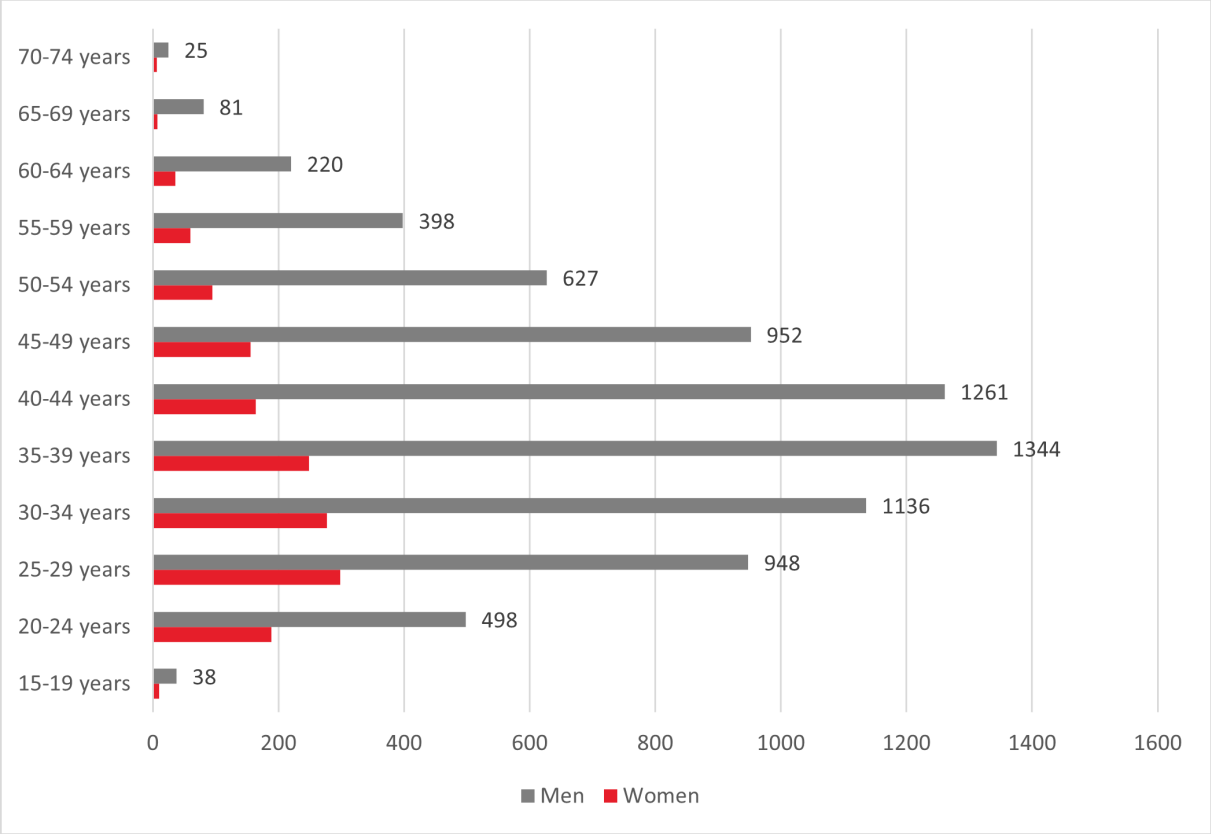
(Source: Author's calculations using ABS, Census of Population and Housing, Table Builder, 2021.)

Drawing on the Census 2021 data, Australia's cyber security workforce – 17 per cent women and 83 per cent men – displays the following demographic and socio-economic characteristics:

- The age profile of female cyber professionals is relatively younger than men's (Figure 5). This suggests that women's representation in the sector is growing through generational change, but it also points towards potential barriers impeding older women from pivoting into entering the sector.
- The employment of cyber security professionals across Australia's states and territories is largely reflective of the general population, with the exception of the ACT's larger share (Figure 6) due to federal government agencies responsible for cyber security being located in ACT.
- Around four in five cyber security professionals are employed in the private sector, while the remaining share is employed in the government sector. These shares are similar for men and women (Figure 7).
- A slightly larger number of migrant workers that have entered the Australian cyber security sector are women. The largest share of these female migrants arrived in Australia in the past ten years (Figure 8).
- Part-time employment is less prevalent within the occupation than it is among the wider workforce, especially among men. Long hours are a feature of the occupation: 18 per cent of men and 14 per cent of women in the occupation work at least 45 hours per week (Figure 9).
- The earnings profile of full-time cyber security professionals shows an over-representation of men in higher income brackets (Figure 10).
- Around 44 per cent of the workforce hold undergraduate qualifications, while another quarter of the workforce hold postgraduate qualifications as their highest level of educational attainment. Women in the sector have a higher level of educational qualifications than men (Table 2).
- Information technology is the most common field of study for cyber security professionals, which also encompasses computer science and information systems. While two-thirds of men in the cyber security sector have educational qualifications in information technology, only around half of all women in the sector specialise in information technology. Women in the sector come from a broader range of disciplinary fields, including business, management and social sciences. Engineering is also a key field of study among cyber security professionals, but it is more common among men than women (Table 3).
- Around 1 per cent identify as Indigenous (Aboriginal, Torres Strait Islander, or both). This share is the same for both men and women.
- Around 0.5 per cent of cyber security professionals indicate that they need assistance with core activities. This is fractionally higher among women.

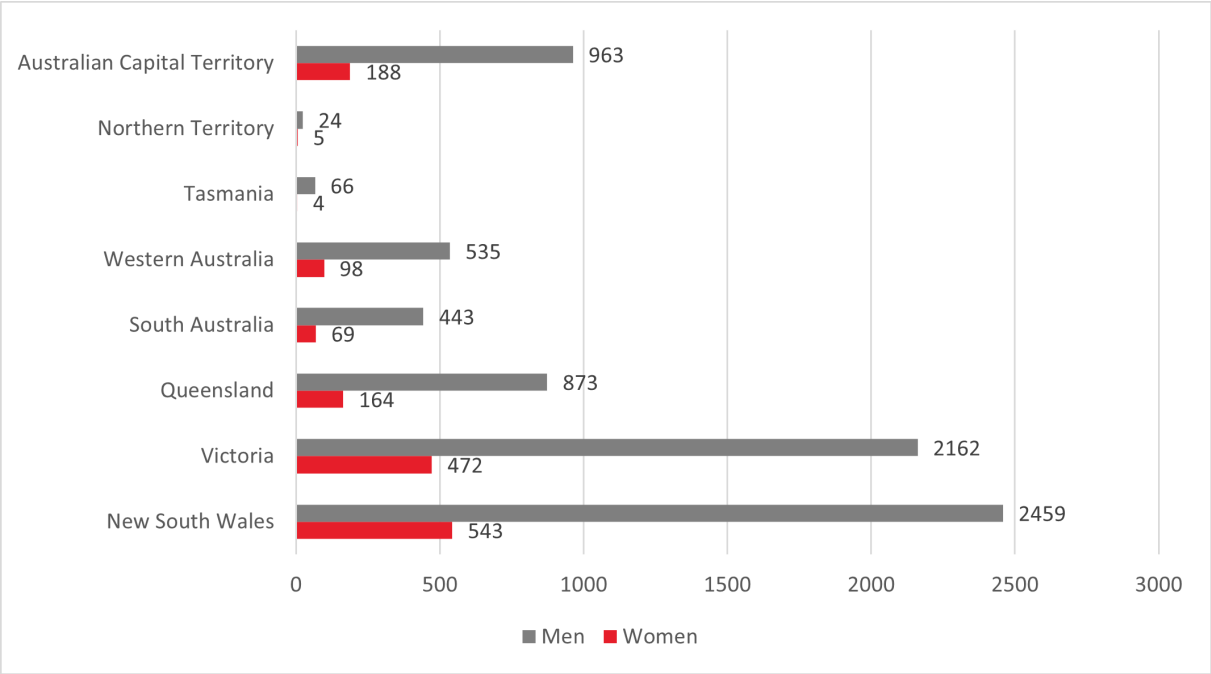
NOTE: The following figures (Figures 5 to 10) and tables (Table 2 and Table 3) examine the demographic make up of the 17 per cent of women and 83 per cent of men that are employed in cyber security occupations in Australia (Figure 3).

Figure 5: Age profile of cyber security professionals, Australia, 2021



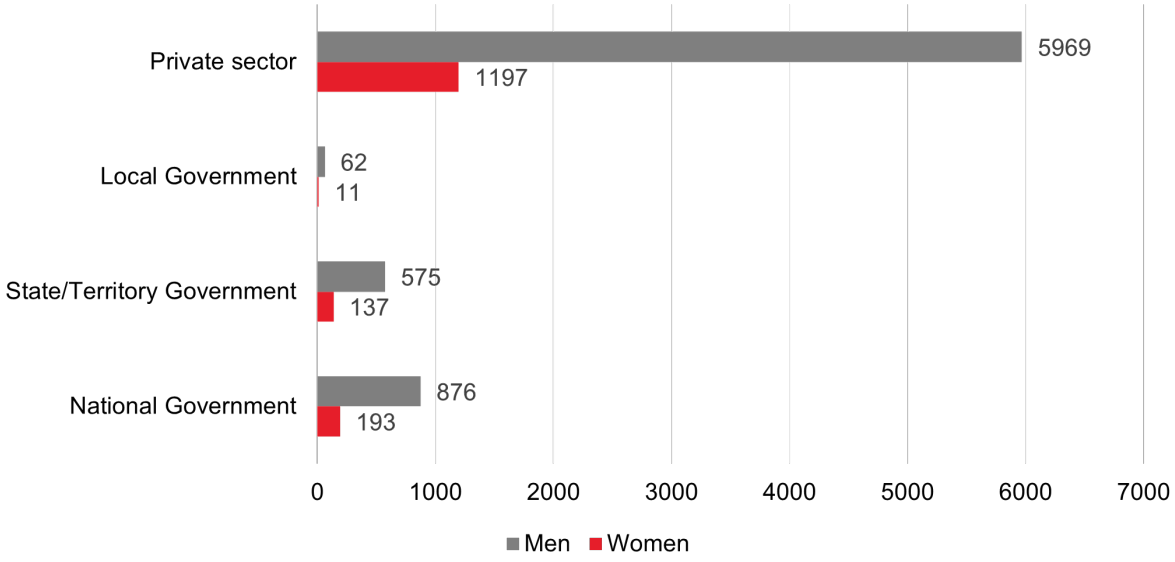
(Source: Authors' calculations using ABS, Census of Population and Housing, Table Builder, 2021.)

Figure 6: State and Territory of employment of cyber security professionals, Australia, 2021



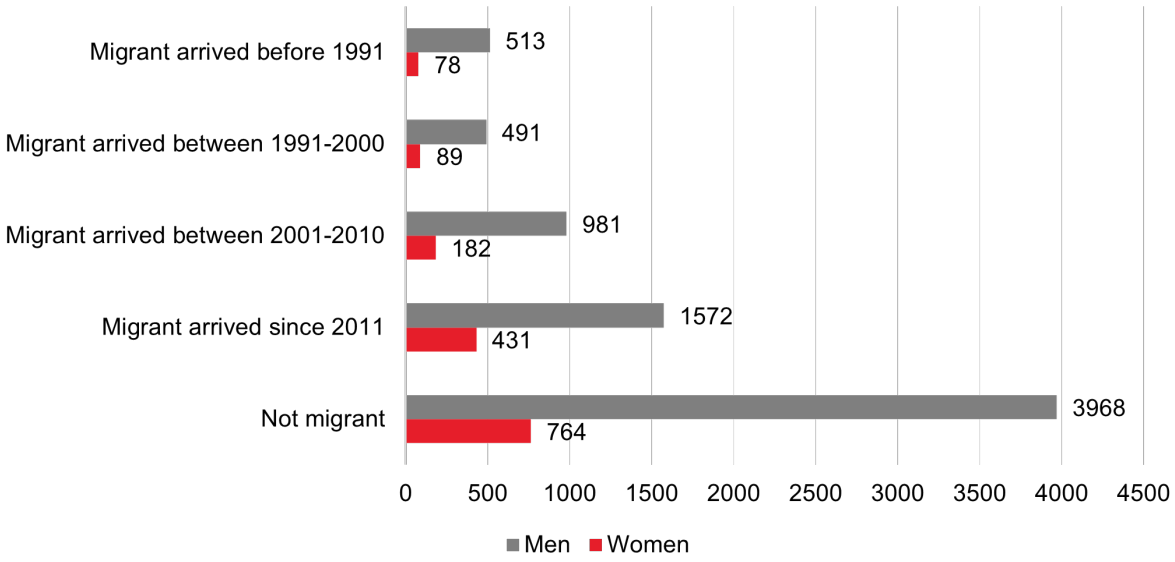
(Source: Authors' calculations using ABS, Census of Population and Housing, Table Builder, 2021.)

Figure 7: Sector of employment of cyber security professionals, Australia, 2021



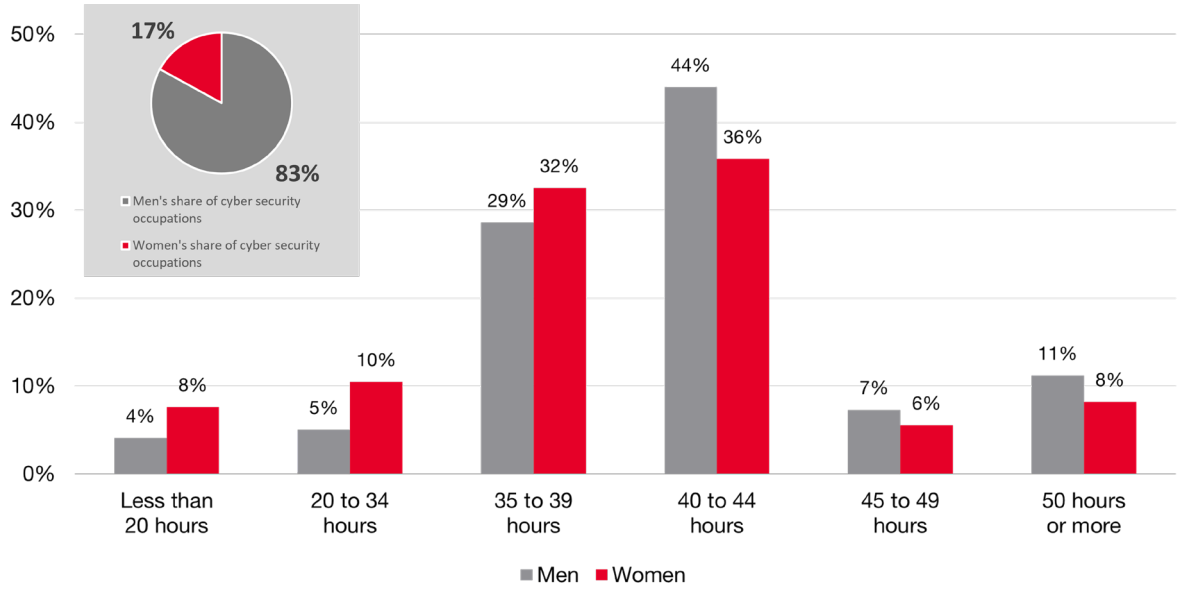
(Source: Authors' calculations using ABS, Census of Population and Housing, Table Builder, 2021.)

Figure 8: Migrant background of cyber security professionals, Australia, 2021



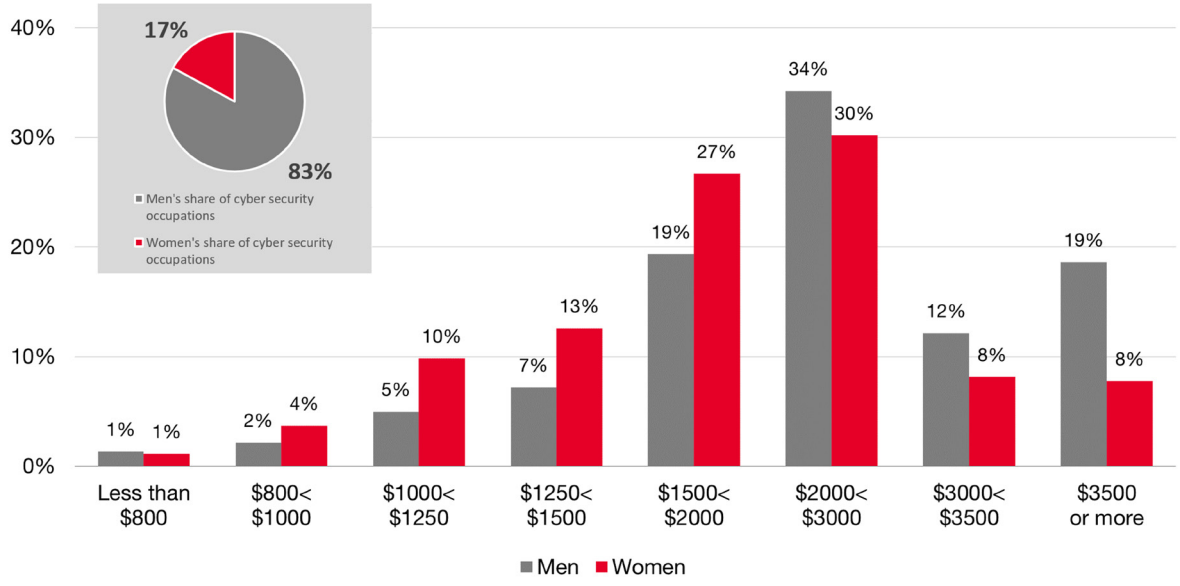
(Source: Authors' calculations using ABS, Census of Population and Housing, Table Builder, 2021.)

Figure 9: Weekly hours of employment of cyber security professionals, Australia, 2021



(Source: Authors' calculations using ABS, Census of Population and Housing, Table Builder, 2021. Percentages for each gender may not sum to 100% due to rounding.)

Figure 10: Weekly earnings of full-time employed cyber security professionals, Australia, 2021



(Source: Authors' calculations using ABS, Census of Population and Housing, Table Builder, 2021. Percentages for each gender may not sum to 100% due to rounding. Data for people employed between 35 to 44 hours per week.)

Table 2: Educational qualifications of cyber professionals, Australia, 2021

Educational qualification	Men	Women
Postgraduate	23%	27%
Graduate	4%	4%
Undergraduate	42%	45%
Vocational	18%	13%
No post-school qualification	12%	11%
Total	100%	100%

(Source: Authors' calculations using ABS, Census of Population and Housing, Table Builder, 2021. Educational qualification refers to a person's highest level of educational attainment. Postgraduate refers to Doctoral or Master Degree; Graduate refers to Graduate Diploma or Graduate Certificate; Undergraduate refers to Bachelor Degree; Vocational includes Advanced Diploma, Associate Degree, Diploma, Certificate III or IV. Percentages refer to the proportion of each gender with the respective qualification.)

Table 3: Field of study of cyber security professionals, Australia, 2021

Field of study	Men	Women
Information Technology	63%	50%
Engineering and Related Technologies	15%	9%
Management and Commerce	10%	17%
Society and Culture	6%	14%
Natural and Physical Sciences	3%	5%
Creative Arts	1%	3%
Education	<1%	1%
Health	<1%	1%
Food, Hospitality and Personal Services	<1%	1%
Agriculture, Environmental and Related Studies	<1%	<1%
Architecture and Building	<1%	0%
Total	100%	100%

(Source: Author's calculations using ABS, Census of Population and Housing, Table Builder, 2021. Field of study is in relation to a person's highest level of post-school educational attainment. Percentages refer to the proportion of each gender within the respective field of study.)

5 Has women's share of the cyber security workforce changed over time?

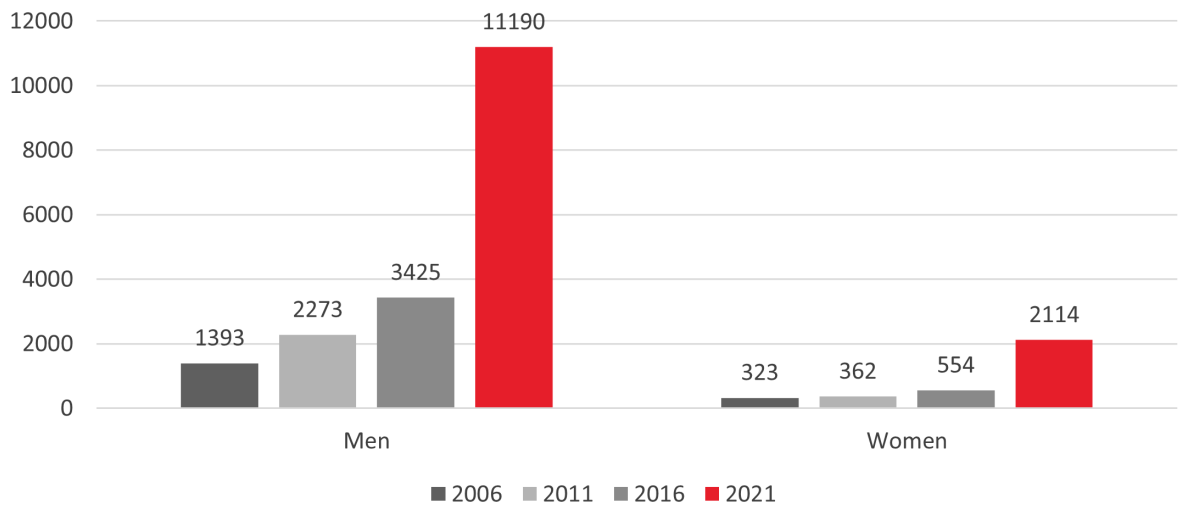
Specific data on cyber security professionals only became available in the most recent Census data collection. Prior to the 2021 Census, the cyber security workforce was mostly counted as part of a broader occupational category called ICT Security Specialists.

The number of people employed as ICT Security Specialists in the Australian workforce has soared in recent years (Figure 11). From 2016 to 2021, the number of ICT Security Specialists in Australia grew by over 200 per cent. Compared to the preceding decade, this is a fourfold increase. The Census count in 2021 found that the number of people working in this occupation now exceeds 13,000 in total.

However, this significant growth is not benefitting everyone equally. The increased importance of the ICT sector and the rapid growth in ICT positions has mainly been a boon to men: As of 2021, women comprised only 16 per cent of all ICT Security Specialists (Figure 12). Despite the efforts of numerous stakeholders, these numbers have stayed more or less identical over the last fifteen years. In other words, this diminutive ebb and flow of women's share in ICT security roles illustrates that most of the newly created positions in recent years have been mainly filled by men.

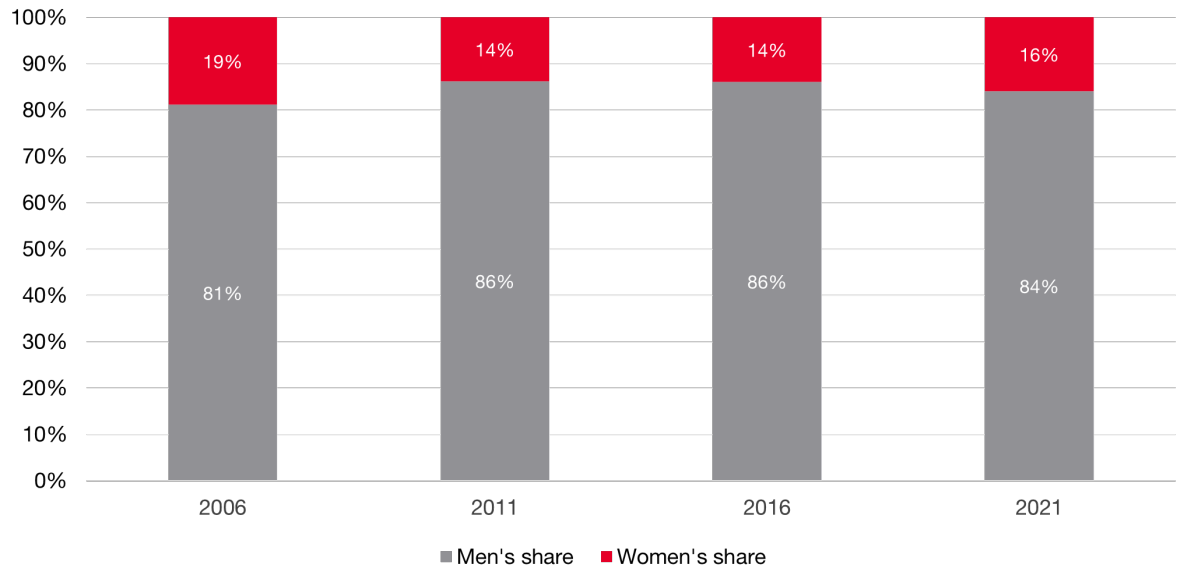
More promising, however, is that the number of women in ICT Security Specialist roles is now officially growing slightly faster than the absolute number of men. In the past five years, women's numbers in ICT Security Specialist roles grew fourfold, while men's grew threefold. Though women's baseline is significantly lower, such continued growth could positively impact gender equity in the sector.

Figure 11: Number of people employed as ICT Security Specialists, Australia, 2006 to 2021



(Source: ABS, Census of Population and Housing, Table Builder, 2006 to 2021.)

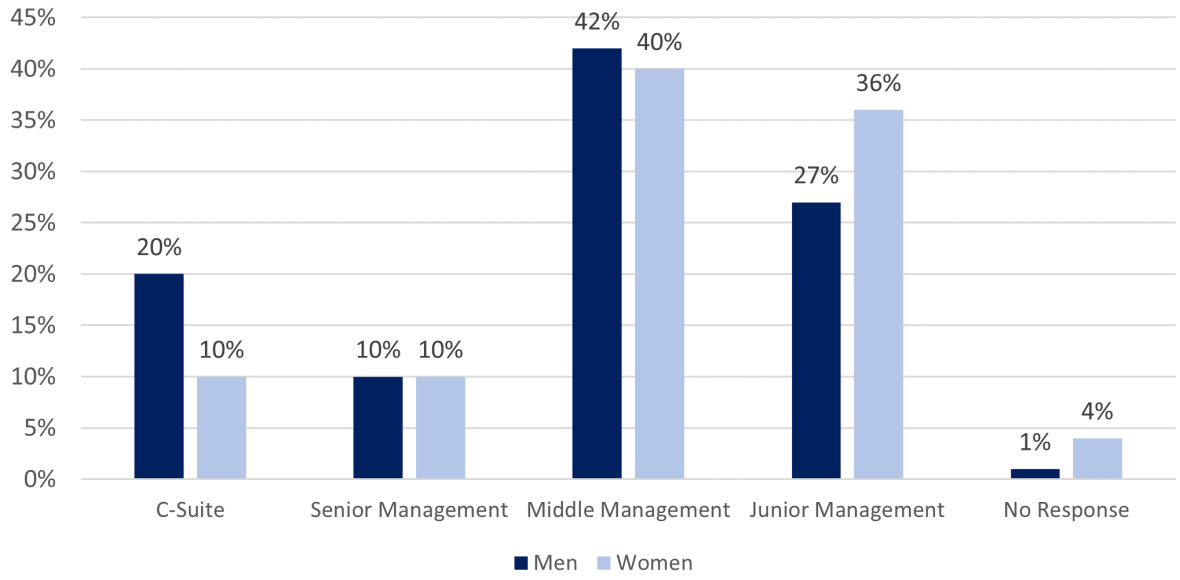
Figure 12: Gender composition of ICT Security Specialists, Australia, 2006 to 2021



(Source: Authors' calculations using ABS, Census of Population and Housing, Table Builder, 2006 to 2021.)

The Australian Security Industry Workforce – Understanding Gender Dimensions survey conducted by RMIT (2022) gives further insight into the proportion of women working in various management levels of Australia's cyber security sector (Figure 13). The respondents were categorised based on their nominated employment title.

Figure 13: Distribution of people employed at management level in cyber security sector, by gender, Australia



(Source: RMIT 2022, Australian Security Industry Workforce – Understanding Gender Dimensions Survey.)

Management levels are categorised into four levels:

- C-suite: leaders who define and develop business strategies and make imperative business decisions.
- Senior management: leaders and managers who implement strategy, vision, and missions of organisations and make decisions, mostly below the C-suite and board of directors.
- Middle management: managers whose role is defined by implementing decisions and ensuring the smooth everyday operations of businesses.
- Junior management: managers and specialists who carry out the daily activities of organisations and who directly or indirectly supervise employees.

Women in management tend to be concentrated in the junior and middle management levels and are severely under-represented at the C-suite level. Women's absence at the upper echelons of management manifests in the everyday decision-making processes of the majority of businesses. That is, strategy development and other significant business plans are more likely to reflect a masculine perspective. Similarly, women's share in junior-level management is disproportionally large. A roughly equal proportion of male and female respondents from the survey sample indicated that they currently worked in middle management or senior management. Some of the reasons for the above representations (Figure 13) are explored in the following sections.

6 What are the experiences of people working in the security workforce?

6.1 The influence of role models and mentors

The RMIT survey explored the influence of exposure to mentors and role models on people's aspirations to enter the cyber security sector and their experiences during their employment in the sector. The gender of the mentor or role model – that is, whether mentees had role models and mentors who were the same gender as them or different – was part of this study.

Mentors usually occupy senior positions and are people who can serve as experienced and trusted advisers to more junior workers in the field. **Role models** can be described as people whose behaviour sets an example to others, who others in the field may look up to as a source of inspiration and instructive exemplars. Others may seek to emulate the role model's career decisions.

The findings showed that there was considerable exposure to role models and mentors by both men and women participating in the survey and that these role models and mentors had a significant influence on all genders at all stages of their careers – from initial training and studies, to making decisions to enter the cyber security sector, to their career aspirations during employment.

The gender of the role models and mentors is skewed towards males, which is a likely reflection of the fact that the sector is predominantly male in composition. That is, women are far more likely to have male mentors and role models than female role models and mentors. Increasing the overall share of women in the sector in more senior roles will lead to greater opportunity for women to find female role models.

6.1.1 Exposure to role models and mentors

Nearly two in five women (39 per cent) and men (38 per cent) participating in the survey reported that they were exposed to role models during their studies and training. A similar fraction – 43 per cent of women and 39 per cent of men – reported that they had mentors during their studies and training.

While employed in the cyber security sector, this rate of exposure to mentors is slightly higher, at 59 per cent of women and 60 per cent of men. Exposure to role models was at 65 per cent for women and 69 per cent for men while working in the sector.

There is still potential to grow and improve mentoring and role modelling opportunities for women and men, both during studies and employment, in order to positively influence career aspirations to enter and remain in the cyber security sector.

6.1.2 Gender of role models and mentors

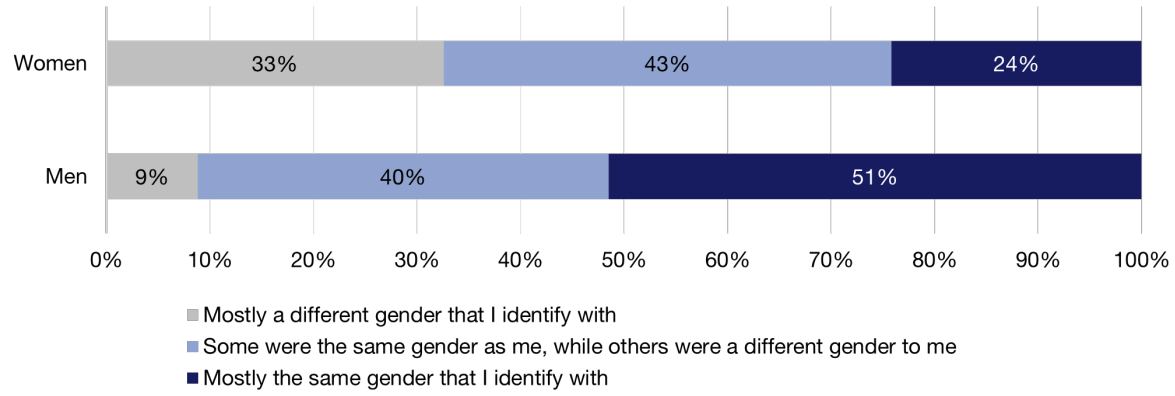
Most commonly, women identified that they did not have role models and mentors that were the same gender as them, meaning the role models and mentors that influenced them were predominantly male.

During their studies and training, only 24 per cent of women had a female role model and 29 per cent had a female mentor, whereas 51 per cent of males had a male role model or mentor (Figure 14 and Figure 15).

The picture is much the same when women are employed in the security industry. During employment, only 27 per cent of women reported having a role model or mentor of the same gender, whereas the figure was almost double for men, with 52 per cent of men reporting having a male role model and 50 per cent reporting having a male mentor (Figure 16 and Figure 17).

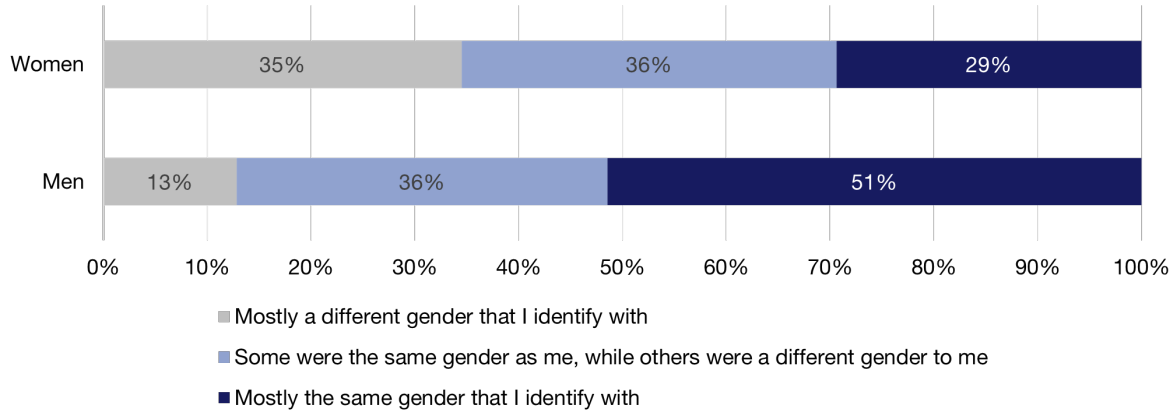
These findings are a likely reflection of women's low overall share of the sector, meaning that female role models and mentors are fewer in number, and therefore less able to be found, compared to men. However, these figures are cause for concern, as research points towards the benefits of mentees identifying for their own gender (Heilman 2012; Ridgeway 2011). This, in turn, can lead to gender-based biases and discrimination in the workplace; undermining the idea of a meritocracy, where individuals are evaluated and promoted based on their abilities and performance.

Figure 14: Gender of role models that influenced career aspirations during studies and training



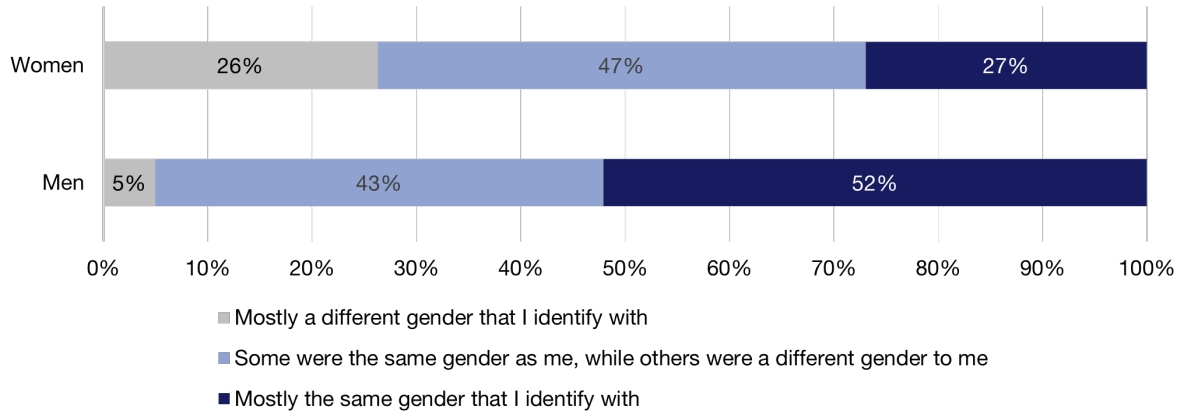
(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions Survey.)

Figure 15: Gender of mentors that influenced career aspirations to enter the security industry during studies and training



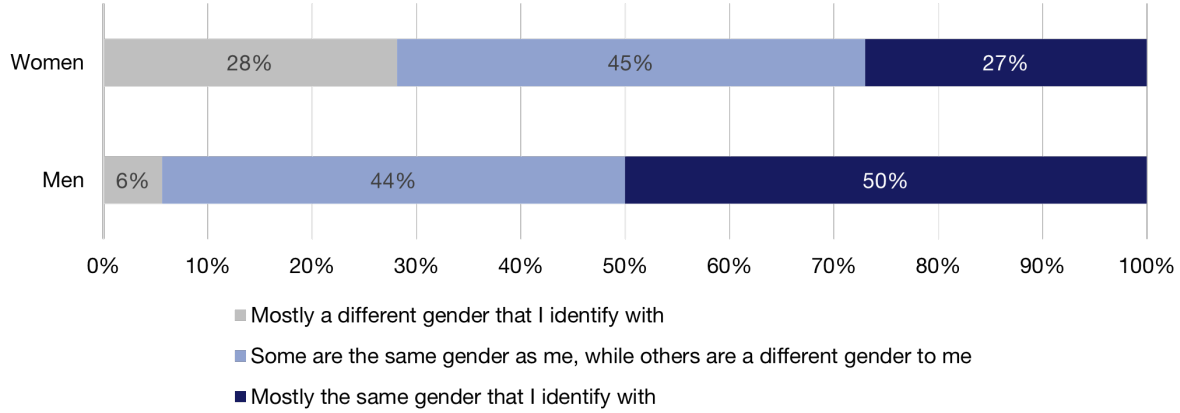
(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions Survey.)

Figure 16: Gender of role models who influenced career aspirations during my employment in the security industry



(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions Survey.)

Figure 17: Gender of mentors who most influenced career aspirations during employment in the security industry



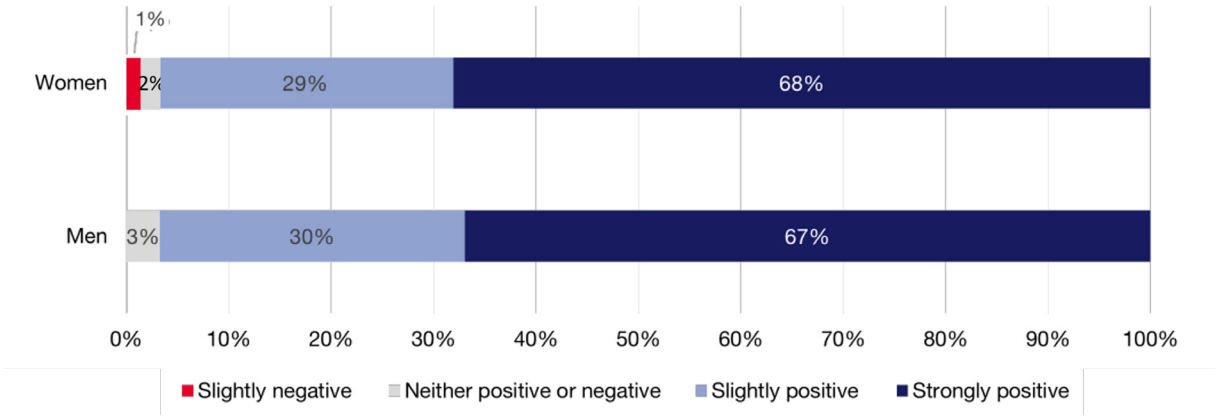
(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions Survey.)

6.1.3 Influence of role models and mentors

Of the survey participants who did have exposure to role models and mentors, survey responses suggested that both men and women were positively influenced (either slightly or strongly) by role models (women 97 per cent; men 97 per cent) and mentors (women 96 per cent; men 98 per cent) while studying and training to enter the cyber security sector. This implies that that mentors and role models have the potential to have a positive influence on the number of women in the cyber security sector.

However, we caution that these survey findings are limited to workers who are currently employed in the sector. Any people who did not have role models and mentors, or were disillusioned by their experiences and left the sector, will not be captured in these survey results.

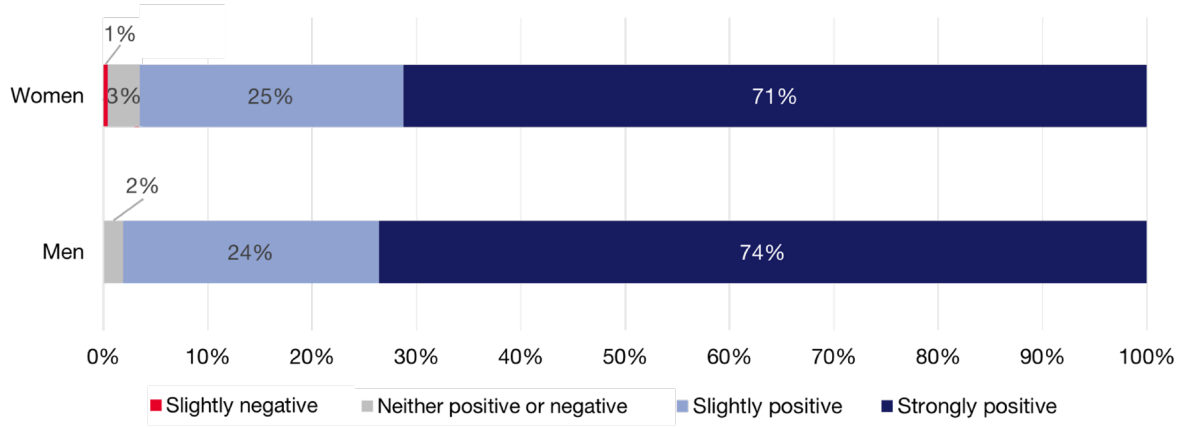
Figure 18: Influence of role models on career aspirations, during employment



(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions Survey.)

In relation to the influence exerted during employment, the role of mentors and role models continues to be an important factor in career development for all genders (Figure 18 and Figure 19). Increasing the number of female role models and mentors in the cyber security sector will likely help retain and attract a more diverse talent pool.

Figure 19: Influence of mentors on career aspirations, during employment

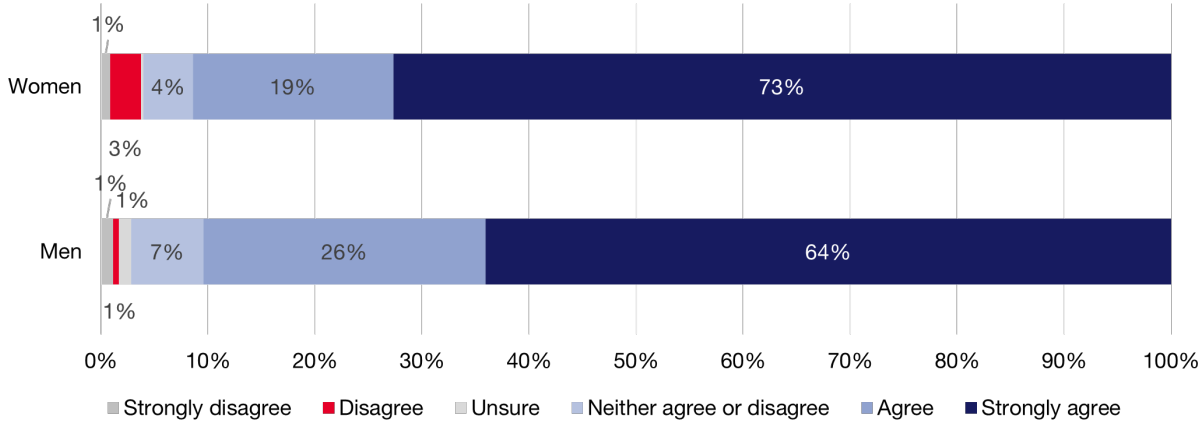


(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions Survey.)

6.1.4 Benefits of investing in gender equity

Participants were asked a series of questions pertaining to gender equity initiatives at work. One of these questions related to whether providing additional support for women to develop their career and whether programs would be beneficial for the industry overall. Strong agreement for this approach was detected.

Figure 20: Perception that additional support for women would be beneficial for the industry overall



(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions Survey.)

The benefits of providing additional support and programs for women's career development was strongly affirmed by all genders. It is promising to observe that all genders express this wider recognition that investing in equity delivers positive improvements for everyone in the sector.

6.2 Motivations for joining the cyber security sector

The workforce survey explored a range of motivating factors that encourage the decision to join the cyber security sector. The motivating factors were segregated between field, study, and industry of choice.

6.2.1 Motivating factors for choosing field of study

This study explores the decision-making factors that influenced men and women who are now working in cyber security when they were at the stage of considering their prospective field of study.

Table 4: 10 most common factors influencing choice of field of study

Rank	Influence	Women	Rank	Influence	Men
1	Job availability	38%	1	Job availability	39%
2	Academic success	37%	2	Academic success	33%
3	Parents	36%	3	Personality	28%
4	Personality	32%	4	Parents	28%
5	Teachers	20%	5	Friends	22%
6	Location (where you live/lived)	19%	6	Creative attributes	19%
7	Beliefs	17%	7	Teachers	18%
8	Friends	14%	8	Internet/social network	16%
9	Mentor	13%	9	Mentor	14%
10	Creative attributes	12%	10	Location (where you live/lived)	14%

(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions.)

Academic success and job availability are the most commonly cited factors affecting students' choice of study, for both men and women. Following these top two factors, the influence of parents appears to be a more common factor for women (36 per cent) more so than men (28 per cent).

While 'friends' ranks as the fifth most common influence on men's decision-making process (22 per cent), it is less influential among women (14 per cent). This implies that women are more strongly influenced by their parents, while men are relatively more influenced by their peers and friends.

Geographical proximity to study options also appears more influential for women than for men. Location is the sixth most common factor (19 per cent) for women and only the tenth most common factor for men (10 per cent).

These findings imply that knowledge about the availability of job opportunities has a strong impact on both men's and women's motivation to choose subjects that led to their careers in cyber security. This demonstrates the willingness of prospective workers to join different industries according to job opportunities or openings in the market. With expanding job opportunities in cyber security sector, the adaptive mindset of this talent pool can be leveraged to help grow and sustain Australia's cyber security workforce.

Given that students are also clearly motivated by their academic experiences, supporting a broader diversity of students to achieve their best throughout their studies in fields that can lead to cyber security careers is also an avenue to invest in.

The factors that were found to be relatively less influential on students' study choices – such as mentoring, which was cited by only 13 per cent of women survey respondents – indicates potential areas where there is opportunity to expand efforts. Even though the influence of teachers was rated as the fifth most common factor influencing women's choices, it was cited by only 20 per cent of respondents. This implies there is more that can be done in the education space, in terms of equipping teachers with resources to actively support their female students to consider career pathways in the field. Given that this is a newly emerging field, it is understandable that some teachers may have limited knowledge about the sector themselves, which is where collaborations between educational institutions and professional organisations are valuable.

6.2.2 Motivating factors for choosing industry in which to work

The RMIT survey asks respondents to identify the motivating factors for their choice of career path. Responses to these questions are shown in Table 5. The factors are listed in the order that they were cited as having the strongest influence on a person's decision to join the cyber security sector.

A quest to make a difference to society was the top influencing factor for both men and women, but even more so among women. Just over half of all female participants (52 per cent) reported that this was their motivating factor for working in the cyber security sector, compared to 44 per cent of men (Table 5).

The next most common motivating factor, for both men and women, was the extent to which they enjoyed studying the academic subjects that related to jobs in the sector. This factor was cited relatively more commonly among men (43 per cent) compared to women (39 per cent), which could also indicate that females were less likely to have a positive experience throughout their studies than men. Their actual performance in the subjects was cited slightly more commonly among men (25 per cent) than women (21 per cent).

The opportunity to fully utilise one's skills was a more commonly cited motivating factor for men (44 per cent) than women (35 per cent). This may indicate that men, more so than women, anticipate that the sector will offer these opportunities to them. If women do not see sufficient opportunity to make full use of their skills, and for their skills and capabilities to be fully valued, this may be a further reason for their reluctance to join the sector.

Job security and employment prospects in the field are also key factors for both men and women, and slightly more so among women.

The role of role models, mentors, family and friends were cited less commonly as motivating factors, but all of these factors were cited slightly more frequently by women than by men. This speaks to the potential gains of investing more strongly in these networks and support structures when aiming to activate female students' interest in the field.

Table 5: Top 10 influences for joining the security industry

Rank	Influence	Women	Rank	Influence	Men
1	I am motivated to make a difference to society	52%	1	I am motivated to make a difference to society	44%
2	I enjoyed the fields of study that relate to the security industry	39%	2	I enjoyed the fields of study that relate to the security industry	43%
3	The sector offers me the opportunity to use my skills	35%	3	The sector offers me the opportunity to use my skills	44%
4	I considered job security and employment prospects in the industry	33%	4	The industry offers opportunities that are suited to my work preferences	35%
5	The industry offers opportunities that are suited to my work preferences	29%	5	I considered job security and employment prospects in the industry	29%
6	I considered earning prospects in the industry	27%	6	I performed well in the fields of study that relate to the security industry	25%
7	I performed well in the fields of study that relate to the security industry	21%	7	I considered earning prospects in the industry	24%
8	I was inspired by role models and mentors who work in the industry	18%	8	I was inspired by role models and mentors who work in the industry	15%
9	I have friends or family who work in the security industry	10%	9	I have friends or family who work in the security industry	7%
10	I could not find other employment options elsewhere	3%	10	I could not find other employment options elsewhere	4%

(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions.)

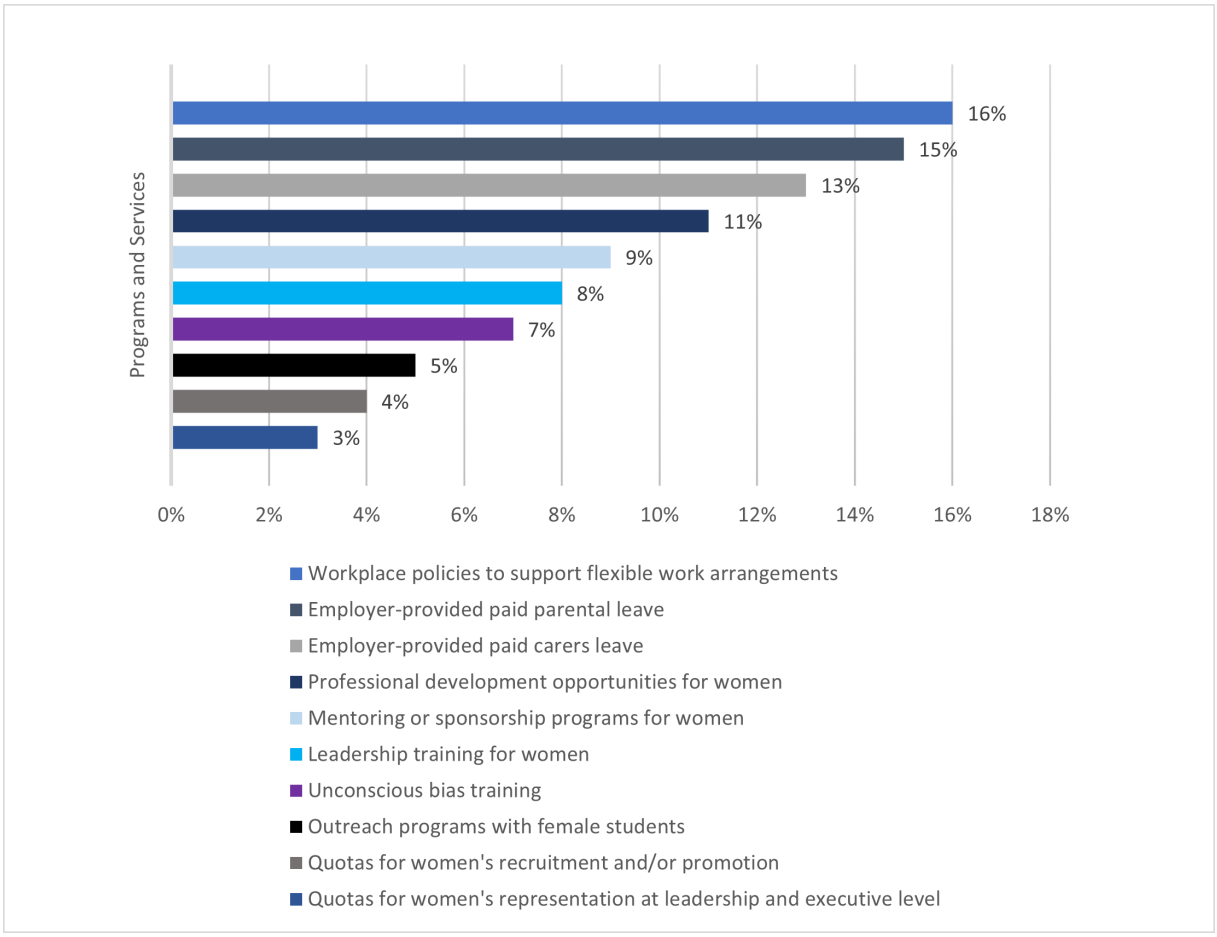
6.3 Factors impacting advancement and retention in the sector

The survey responses provide insight into some of the factors that attract and retain women to the cyber security sector and equitably support their career advancement.

6.3.1 Workplace initiatives to promote gender equity

In the survey, respondents were asked to think about their current job in the cyber security sector and whether the organisation that they work for provides any programs or services aimed at fostering gender equity, supporting women's participation and women's career progression. The most common services, programs and practices that are designed to support women's participation and facilitate career development were identified.

Figure 21: Most common programs and services organisations provide to foster gender equity, supporting women's participation and career progression



(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions Survey.)

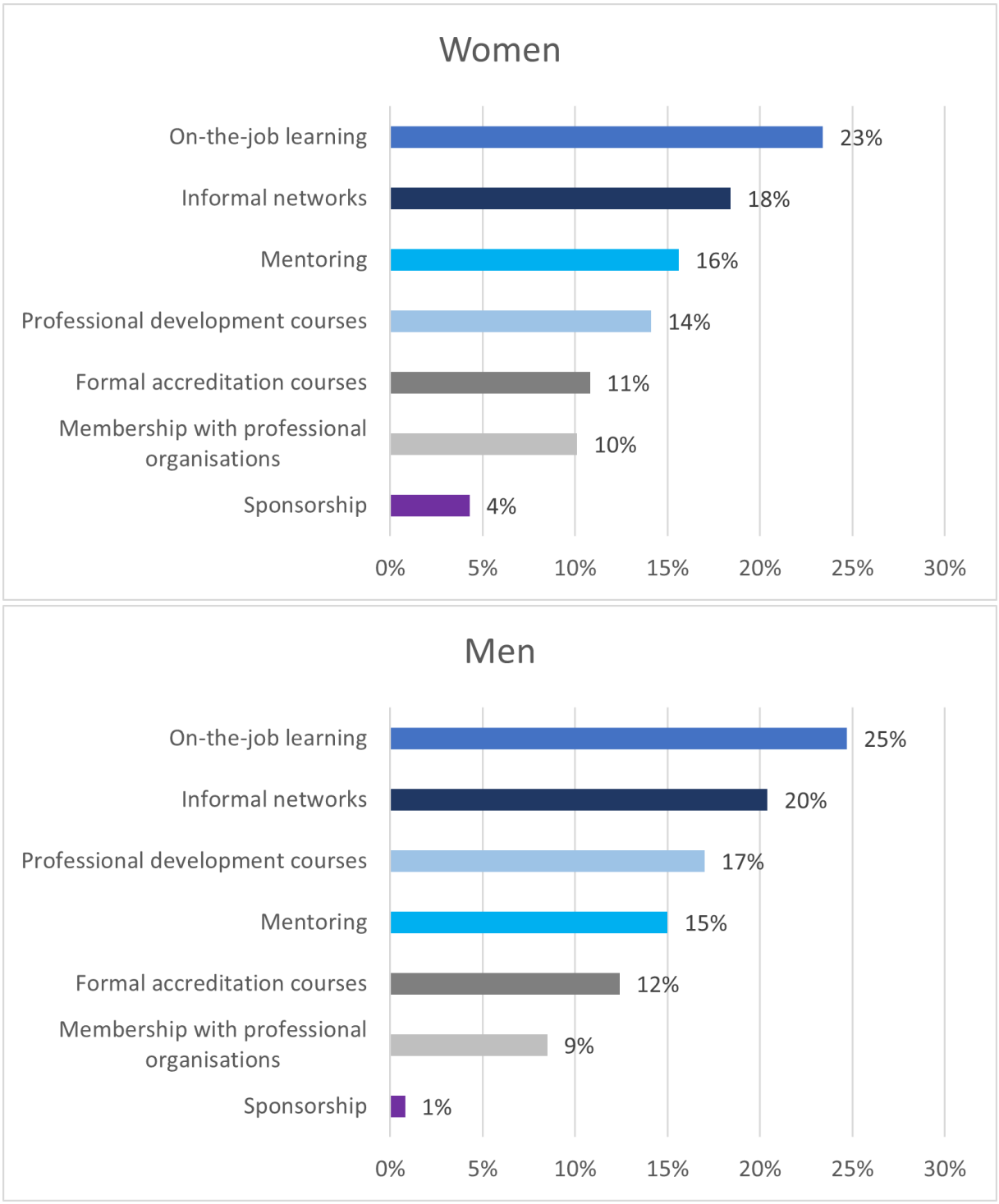
The survey results provide a picture of how commonly these strategies are available from the perspectives of survey respondents. The finding that, at most, 16 per cent of cyber security professionals have one of these gender equity policies available to them, suggests that the majority of employers in the sector do not appear to be investing in such initiatives. These initiatives have the potential to improve women's attraction to and advancement in the workforce. Concentrating on these facilitators could provide pathways for the cyber security sector to improve talent management for women. However, it is also essential to robustly evaluate the impact of each of these approaches in the context of the cyber security sector to identify their relative effectiveness, and the sector needs to invest resources towards these types of evaluations.

Conversely, the absence, or lack of effectiveness, of these facilitators can contribute to the cyber security sector missing out on female talent. Women may be deterred from joining the sector or staying in it because they face barriers, biases, and hurdles once they are in the sector, that their male colleagues are less likely to encounter.

6.3.2 Factors aiding career advancement

To further explore what factors contribute to a person's career advancement in the security industry, we asked participants to identify the professional activities that led to their career advancement. Such insights may generate practical knowledge for the cyber security sector and recruiters.

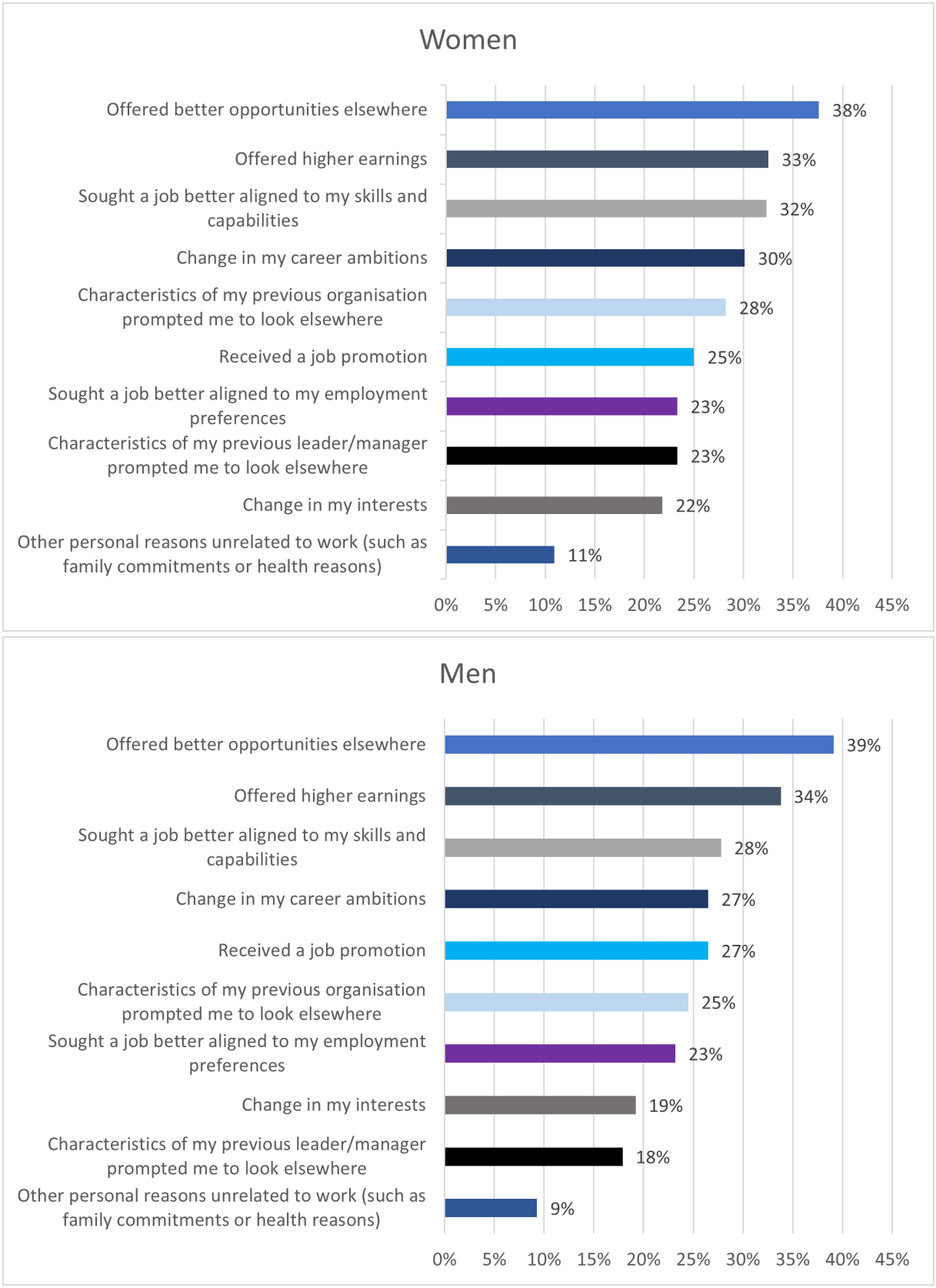
Figure 22. Professional activities that have specifically aided your career advancement in the security industry



(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions Survey.)

Both male and female respondents indicated that they benefitted the most from on-the-job learning, informal networks and mentoring. These results emphasise the need for inclusive networking opportunities for women. Formal professional development activities (e.g. formal accreditation courses) are also identified as important professional activities that can aid career development among women.

Figure 23: Most common reasons for most recent job change



(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions Survey.)

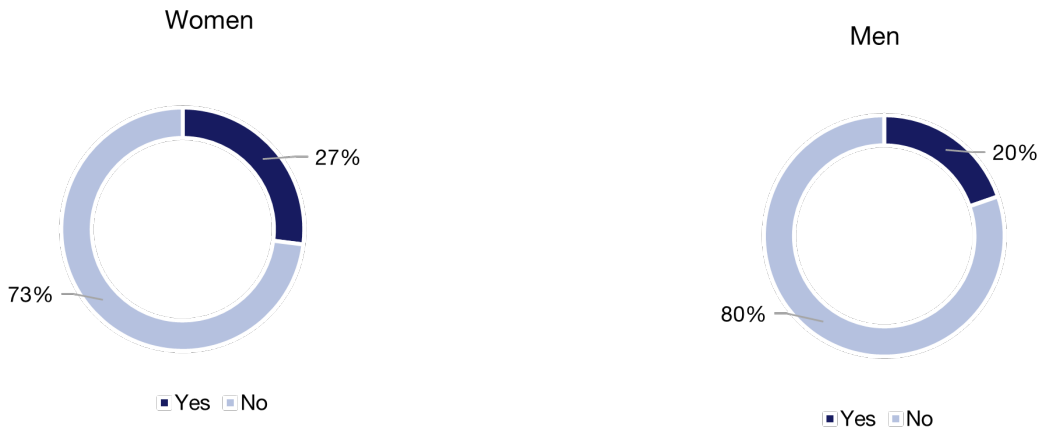
The most common reason for changing jobs – for men and women – was being offered better opportunities at a different organisation.

Survey participants indicated that the main reasons for their most recent career change were mostly of a positive nature: job promotions, higher earnings, and better opportunities elsewhere (Figure 23).

6.3.3 Career breaks

It is well known that, within the workforce more generally, women experience more career breaks due to childrearing and gender patterns in caring responsibilities. This study explored the extent to which men's and women's workforce attachment differs within the cyber security sector.

Figure 24: Breaks taken in paid employment during career in security industry



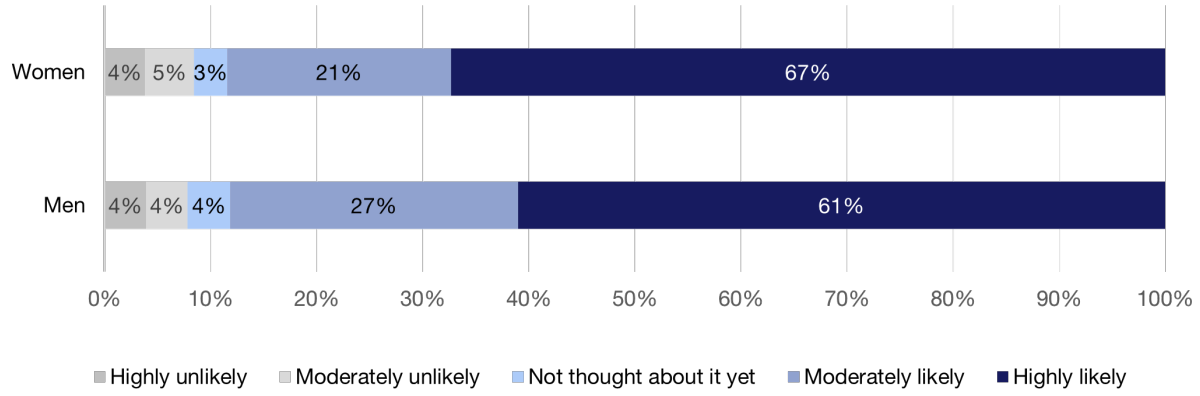
(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions Survey.)

Figure 25: Duration of breaks taken in paid employment during career in security industry

(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions Survey.)

The survey identified gendered differences in the duration of career breaks. More than 40 per cent of women are likely to take a career break longer than 12 months. Ten per cent of women took breaks between 3-5 years and more than 2 per cent of women indicated that their longest break lasted over five years. By comparison, the data indicates that only 23 per cent of male respondents took a break longer than 12 months, and none indicated that they took a break longer than 2 years.

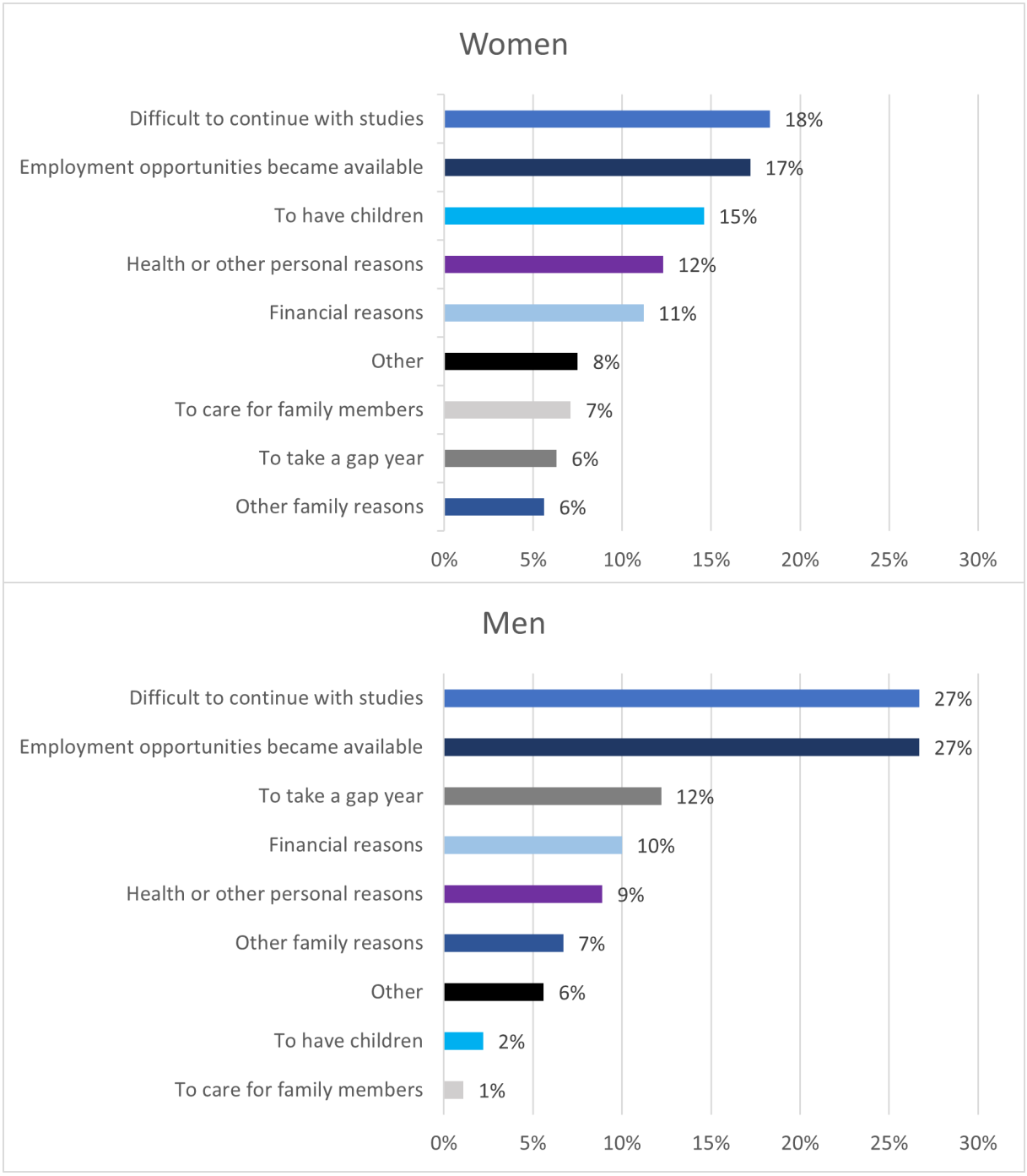
Figure 26: Percentage of respondents that expect to be working in the security industry in the next five years



(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions Survey.)

The cyber security sector has an opportunity to nurture and sustain the current female talent pool, as 67 per cent of female respondents expect to be working in the cyber security sector for the next five years (compared to 61 per cent of male respondents). This can be done by responding strategically to the potential factors indicated by the survey participants (Figure 27).

Figure 27: Reasons for break or interruption to studies or training



(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions Survey.)

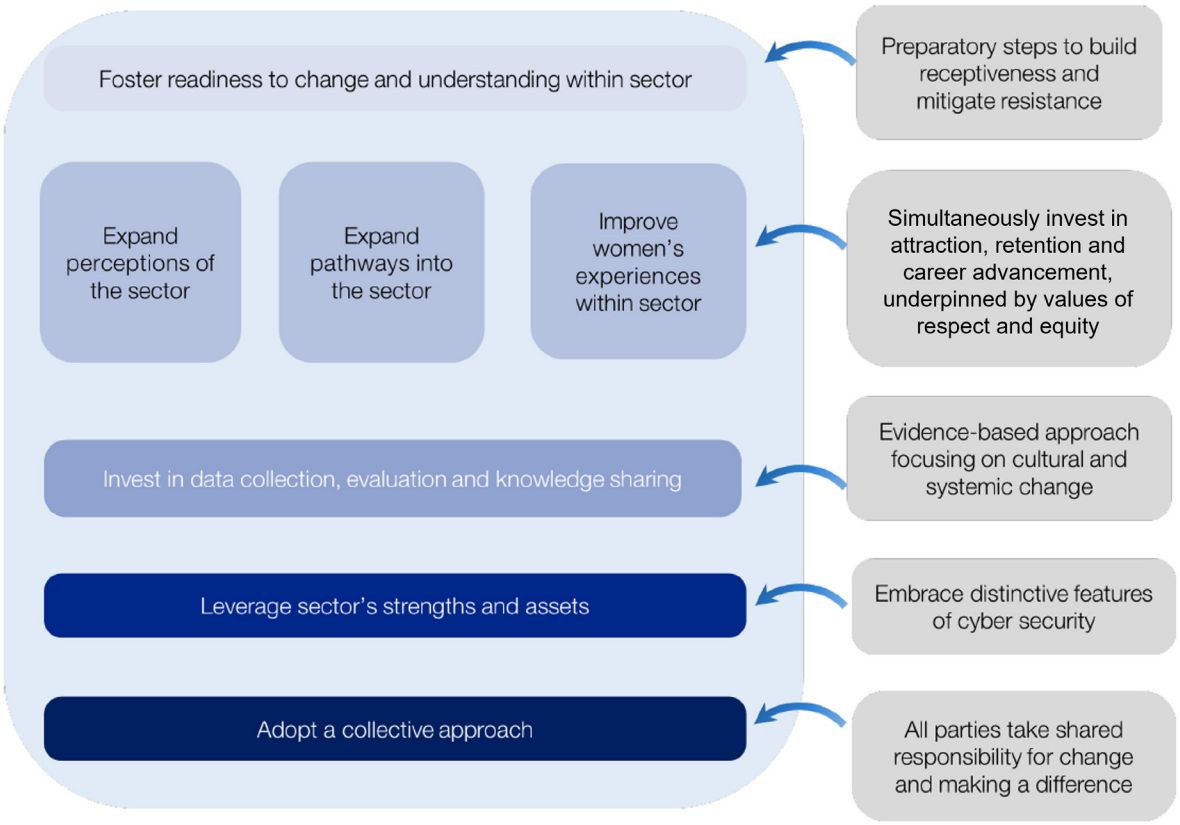
Worthy of note here is that caring and family reasons are the main reasons for breaks and interruptions for female participants when the reasons 'to have children' and 'to care for family members' are combined (22 per cent). Women's percentage is considerably higher (15 per cent) than men's (2 per cent) for taking a break to 'have children'. Similarly, 7 per cent of women and 1 per cent of men are taking a break 'to care for family members'. One might reasonably expect some gendered differences to arise here, yet it must be acknowledged that the societal onus to care for children and family members is still placed on women.

Given that female talent in the cyber security sector is quite scarce (Figure 3; Figure 11) it is important to look at women's expectations about staying in this sector and the factors that can impact their decision-making.

7 What can be done to create a more gender inclusive workforce?

Insights from this research are combined with emerging evidence on best practices so that pragmatic steps for a more gender equitable and inclusive workforce can be established. In this way, the cyber security sector is able to adapt and tailor gender equity strategies that have proven to be successful in other sectors.

Figure 28: Steps towards gender equitable and inclusive cyber security sector



7.1 Foster readiness to change and authentic understanding within the sector

Creating a diverse and inclusive workforce is not only imperative to an organisation's ability to innovate, but such a strategy is also a reflection of an organisation's values and principles. Research shows that fostering genuine awareness and understanding of the existence and influence of gender biases can improve a workforce's receptiveness to the implementation of gender equity and diversity initiatives (McKinsey 2018).

Therefore, it is important to understand the existence of implicit bias and to create awareness of the need for cultural change. This includes communicating the benefits of change and addressing resistance.

There are some positive indications of receptiveness towards equity initiatives in the cyber security sector. The RMIT survey found that the majority of women and men strongly agreed that gender equity initiatives would be beneficial for the development of women's careers in the cyber security sector (see Figure 20).

7.2 Expand perceptions of the sector

There is a pressing need to **dismantle stereotypical images and narratives** of the cyber security sector. Stereotypical images of men as "natural" leaders still prevail, and the cultural belief in Australia that computer science is a domain for men act to deter women from entering the security sector (Michell et al., 2017). These perceptions discourage girls and women from entering the sector, cause imposter syndrome, and create work environments in which work sexual harassment prevails.

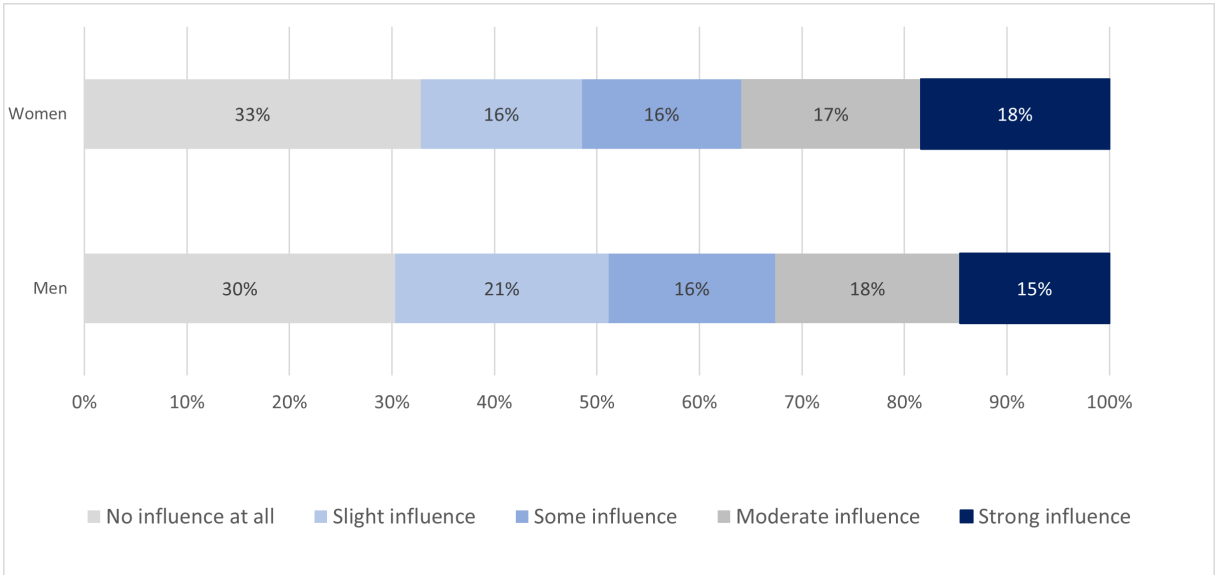
Computer science is often labelled as "nerdy" by popular culture (Cheryan et al., 2013). Such representations cause impressionable minds to believe that these nerdy characteristics of scientists are typical and are therefore prerequisites to entering STEM fields. It is necessary to **broaden the image of computer science** through the internet and media by establishing a much more inclusive image of scientists and breaking the stereotype of the "geeky technician". This would be instrumental in disseminating an open, attractive image of the cyber industry that would be appealing to today's girls and women.

Examples of sexist work cultures that perpetuate gendered stereotypes and incidences of bias, sexism, and sexual harassment include:

- Employer recruiting tactics that highlight the male-dominated culture of the tech industry and which potentially deter women from pursuing employment with those companies.
- Microclimates within teams proving to be detrimental even though the hiring organisation's overall culture and initiatives are inclusive.
- Gender composition in a workplace that creates an imbalance and a "minority status".
- A culture that creates a general acceptance that there is a low expectation of women.
- Male bonding rituals that exclude women creating a lack of bonding with male peers, coaches, and supervisors (Lapan & Smith, 2022).

In the RMIT survey, 50 per cent women mentioned that they were inspired by **role models and mentors** who work in the security industry to join the industry.

Figure 29: Impact of role models and mentors who work in the industry to join the security industry



(Source: RMIT 2022, Australian Security Industry Workforce - Understanding Gender Dimensions Survey.)

This data confirms that exposing women and girls to role models and mentors is essential to break down gender-stereotypical beliefs on STEM interest and engagement (De Gioannis et al., 2023). It is therefore reasonable to infer that early exposure to role models and mentors should be a priority for education institutions and the industry.

The significance of the **influence of parents and family factors** in shaping aspirations of children and their choice of higher education (Lloyd et al., 2018) is also demonstrated in the RMIT survey. 36 per cent of women mentioned that parents played a significant role in their choice of field of study (Table 4). The path forward is to educate parents and develop their awareness of STEM, computer science and cyber security and how these fields can transform their children's lives.

7.3 Expand pathways into the sector

Formal and informal networks are critical. The RMIT survey indicates that such networks have a significant influence on career advancement (see Figure 22). This finding points towards the value of expanding resourcing for women to build their informal networks through, for example, professional industry organisation membership and networking opportunities, internships, and mentoring programs. Such networks can have a profound impact on a woman's career choice and their decision to continue on a particular career path. In addition, networking opportunities and events need to be structured in a way that is inclusive to women (for example, the timing and nature of team activities and events do not conflict with family responsibilities).

Successful **mentoring** is an essential pathway to developing, nurturing and sustaining women in security and cyber security sectors (Saffie-Robertson, 2020). Role models can have a significant impact on women employed in male-dominated sectors and on employees who are part of minority groups (Ng & Rumens, 2017; Tokbaeva & Achtenhagen, 2021). Research highlights the overall value of having mentors and role models with whom mentees can identify, as this increases the results of the effectiveness of the mentoring relationship (Saffie-Robertson, 2020; Torres-Ramos et al., 2021). This is reinforced by the RMIT survey, where the influence of mentors and role models is highly regarded by all genders. However, women do not currently have equal access to role models and mentors of the same gender as men do. Formalised mentoring programs offered by industry associations and businesses play a key role in providing a positive influence on women's careers in the security sector. These programs should continue to be offered and, if possible, expanded to create further opportunities for women.

Another means by which pathways into the sector can be expanded is by facilitating flexibility for women to pivot into the cyber security sector later in their careers. Over 50 per cent of women respondents to the RMIT survey have indicated that they have moved into the security industry in the last five years from another industry or occupation. Also, over 50 per cent of women respondents did not study a technical cyber-related field of study. These survey findings highlight the need to **invest in opportunities for reskilling and upskilling**, as well as improved systems for the recognition of the transferability of existing skills and previous career experience from other industries.

7.4 Improve women's experiences within the sector

The focus on improving women's experiences in the cyber security sector needs to make fundamental shift from "fixing women" to "fixing the system" (Bohnet 2016; Fox, 2017). Without doing this, the sector will not be able to effectively address gender bias.

Creating a more gender balanced workforce is about far more than simply encouraging more women to study IT and hiring more women. It's about recognising the reasons why women – even if they enjoy the field of study and aspire to join this field – are deterred by aspects of the workforce culture and are disadvantaged by inequities within workforce systems. There are a number of strategies that employers can use to reframe their workforce culture, policies and practices and make their organisations more attractive and suitable for women.

Create a culture that recognises and values women's capabilities, as well as the other factors that women are disproportionately affected by due to existing gender patterns in households and society (such as the likelihood that women have a greater responsibility for caregiving for family members).

Create a more gender equitable culture that respects and **supports workers with caring responsibilities.** This includes supporting more men in the sector to take on caregiving roles, through, for example, the provision of parental leave for fathers and moving away from a culture where employees work excessively long hours. Workers who take on care responsibilities also need to be assured that they will not encounter repercussions or penalties for doing so, such as being overlooked for promotional opportunities or facing assumptions from employers that question their commitment to their career.

Put in place **organisational policies and practices that support all workers** to balance work and care responsibilities, and that address the pressure and expectation on workers to work long hours (which can be ostracising for workers with caring responsibilities). For example, during a cyber attack, it is common for individuals and teams to work extended hours to contain the attack and prevent further damage. The urgency and critical nature of a cyber attack often requires a rapid response, which may involve working around the clock until the situation is resolved.

While gender equity initiatives tend to focus on providing role models for women, it is equally important to **provide role models for men** who champion and promote respectful and inclusive behaviour.

Ensure **equitable salary and benefits and equal access to opportunities.** Employers need to undertake gender pay gap analysis to identify and monitor instances where women are being paid less than male peers of comparable occupational rank and responsibilities.

Eliminate toxic work cultures and adopt a positive duty of care to all employees that fosters respect, equal opportunity and inclusion, and that eliminates toxic behaviour such as harassment, abuse, and discrimination.

The survey data shows an over-representation of women in entry level roles. However, given the recent influx of women into the cyber security sector, the sector is now well-placed to drive gender equity through the development and promotion of women. This can be achieved through initiatives such as **women's leadership programs and career mentoring.** This is particularly important given that the survey analysis also shows an over-representation of men at senior levels. The income profile of cyber security professionals, based on Census data analysis, confirms that a disproportionate share of men are in senior, higher-paid roles.

While **flexible work arrangements,** such as remote work and working-from-home, have generally been a feature of the IT sector for some time, human resource practices need to ensure that those who work from home and/or work part-time are not disadvantaged, and are given equal opportunity for career development and progression.

The survey results also indicate that 3 per cent of respondents identified as non-binary, gender-fluid or gender-diverse. This level of response made it difficult to draw meaningful conclusions from the data for this particular group. Consequently, this presents an opportunity to conduct detailed research in the future relating to non-binary individuals working in the security industry to explore in detail their specific experiences and to examine the factors that would enable a more diverse and inclusive workforce.

7.5 Invest in data collection, evaluation and knowledge sharing

Many organisations do not currently measure their gender equity programs and initiatives (McKinsey 2018a), and as the saying goes, 'what does not get measured does not count.' It is critical that organisations invest in data collection, measurement and evaluation and that they understand the effectiveness and impact of any gender equity initiatives that they implement to achieve a more gender equitable and inclusive workforce.

Data collection, evaluation and measurement are critical to the success of gender equity initiatives because they provide a way to track progress and determine the effectiveness of specific initiatives. This is important because without data and measurement, it can be difficult to determine whether the initiatives are achieving their goals and making a meaningful impact on gender equity in the cyber security sector. Having data and measurements in place also helps organisations to make data-driven decisions, allocate resources more effectively, and ensure that initiatives are working to achieve their goals.

Following are some of the measures that can be used to evaluate the effectiveness of gender equity initiatives.

Figure 30: Measures to evaluate gender equity initiatives

These measures provide a range of data that can be used to assess the effectiveness of gender equity initiatives and to identify areas for improvement. They also provide a baseline and a way to monitor progress over time and assist in making informed decisions about the allocation of resources to support gender equity initiatives.

It is highly recommended that a **framework of measures** for organisations in the cyber security sector be developed to assist organisations in meaningfully measuring gender equity initiatives and programs.

It is also important for organisations and the industry more broadly to continue to raise the need for gender equity in the cyber security sector. It is imperative that a platform is provided for organisations and industry to share knowledge.

Knowledge sharing promotes diversity and inclusion, fosters a supportive community, increases understanding and awareness of the challenges faced by women in cyber security, and supports professional development and career advancement. By sharing knowledge and promoting an open dialogue, organisations can work together to break down the gender gap and build a more diverse and equitable sector.

Practical ways in which knowledge can be meaningfully shared between organisations and across the industry should be investigated to ensure effective knowledge sharing and high levels of engagement. For example, approach industry associations to include a **gender-focused stream at national cyber security conferences**.

Measurement and knowledge sharing about gender equity can provide valuable insights and perspectives that can inform policies and practices aimed at increasing the representation of women in cyber security. By measuring gender equity and sharing knowledge, while fostering an inclusive culture, the sector can work together to build a more diverse and equitable field and close the gender gap.

7.6 Leverage the sector's strengths and assets

The cyber security sector is uniquely poised to make greater progress on gender equity than other male-dominated fields.

A first point of distinction of the cyber security sector that gives it an advantage in progressing towards gender equity compared to other male-dominated fields, is that **the sector is adaptive, iterative, forward-looking, and innovative** by nature. These characteristics translate to pragmatic action and indicate that the sector is more likely to be willing to evolve and less likely to be constrained by traditional conventions that aim to preserve the status quo. This demeanour has proven to be a key element that makes a difference to achieving progress on equity, diversity and inclusion.

The second distinctive feature of the sector is that in the early 1980s **women's trajectory in computer science** was on the rise. Research suggests that the introduction of computers into households, and the marketing of computers towards males, especially through video games, has had the effect of alienating females from the field (Henn, 2014; Margolis and Fisher, 2003). Census data shows that female participation in ICT Specialist Security roles is now growing faster than male participation.

There is a growing body of research that indicates that a **gender-diverse management team has a positive impact** on productivity, decision-making, financial performance and process and product innovation (Ruiz-Jiménez & del Mar Fuentes-Fuentes 2016; HR Management International Digest, 2019). As this becomes more widely acknowledged and accepted, the cyber security sector is well-positioned to move towards greater inclusiveness.

The fact that the cyber security sector is a **rapidly growing workforce** means that the sector has a promising opportunity to take action now to shape its culture to be one that is gender equitable, inclusive and embracing of diversity, rather than allowing traditional stereotypes to take hold and become embedded within the workforce.

The cyber security sector's strengths outlined above are a formidable asset on which the sector can capitalise. There is a growing awareness of the importance of gender equity, diversity and inclusion in cyber security. Organisations and industry need to provide the means for women to enter and succeed in this field and help break down traditional gender barriers.

Ultimately, the key steps that need to be taken to ensure a more inclusive cyber security workforce for women are to:

1. Change perceptions of the sector;
2. Expand pathways into the sector, and
3. Improve experiences within the sector.

This can be done by committing to actioning the recommendations provided in this report in an effort to increase the representation of women and other under-represented groups.

7.7 Adopt a collective approach where everyone plays a role

All parts of the cyber security sector have a role to play in promoting cultural change and breaking down gender bias. There is potential for all parties to take practical action and make a positive impact on gender equity and inclusion in the sector:

- **Leaders of organisations** can promote cultural change and break down gender bias by setting the tone for diversity and inclusion, promoting diversity and inclusion policies and practices, fostering an inclusive culture, and advocating for change. They can ensure that the organisation's vision, mission, values, strategy, and policies explicitly acknowledge and action diversity. Leaders need to demonstrate their own readiness to learn and openness to do things differently. They can also include gender equity outcomes in executive Key Performance Indicators (KPIs).
- **Organisations** can take a lead in promoting diversity and inclusivity by setting clear goals and targets, implementing diversity and inclusion policies, practices, and programs, and creating a supportive and inclusive work culture and environment. This approach also requires organisations to be proactively alert to resistance against gender equality initiatives, and take steps to understand and diffuse any opposition towards such initiatives, as part of building a workplace culture that is authentically embracing of gender equity.
- **Industry associations** can play a role in promoting diversity and inclusion by creating programs and initiatives that support women in the cyber security sector, by improving the visibility and voices of women in the sector, by ensuring equal representation on boards and committees, by aiming for gender balance and diversity on speaker panels, and by generally advocating for gender equity in the workplace.
- **Education institutions** can help to promote diversity and inclusion in the cyber security sector by ensuring that their curriculums are inclusive and representative, by analysing education content for gender bias and stereotypes, and by supporting initiatives that encourage women and under-represented groups to pursue careers in the sector. They can build informal and formal networking opportunities which will improve awareness and create a support system not only for students, but also for families.
- **Governments** can implement policies and initiatives that support diversity and inclusion (for example, apply gender equity conditions to procurement policies), provide funding and resources for initiatives that promote gender equity in the workforce, support initiatives that encourage women and under-represented groups to pursue careers in cyber security, and invest in programs that provide training and support for employees in the sector. There is scope for governments at all levels to bring a gender lens to policymaking processes more widely, as a way of ensuring that gender equity considerations are part of all policy design, expenditure and budget decisions.
- The **wider community** can create support systems through informal and formal networking opportunities using awareness programs, media coverage and web content, thereby ensuring an ongoing circulation of awareness, knowledge and education. In media, advertising and popular culture, community members can call out gender stereotypical images of the sector and can replace these with more diverse representations.

By working together, all parts of the cyber security sector can help create a more inclusive and diverse industry culture, breaking down gender bias and promoting gender equity.

References

1. Artz, B, Goodall, AH & Oswald, AJ 2018, 'Do women ask?', *Industrial Relations,* 57(4): 611-636.
2. AustCyber 2020, *Australia's Cyber Security Sector Competitiveness Plan 2020,* Australian Government Department of Industry, Science, Energy and Resources, https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2020.
3. AustCyber Explorer 2022, Supply & Demand Maps, AustCyber Explorer, https://www.aucyberexplorer.com.au/maps/current-supply-demand.
4. ABS (Australian Bureau of Statistics) 2022, *Australian and New Zealand Standard Classification of Occupations (ANZSCO)*, https://www.abs.gov.au/statistics/classifications/anzsco-australian-and-new-zealand-standard-classification-occupations/latest-release.
5. Australian Bureau of Statistics (various years), *Census of Population and Housing*, TableBuilder Australia, Commonwealth of Australia.
6. Australian Computer Society (ACS) 2019, *Australia's Digital Pulse 2019*, https://www.acs.org.au/insightsandpublications/reports-publications/digital-pulse-2019.html.
7. Australian Computer Society (ACS) 2022, *Australia's Digital Pulse 2022,* https://www.acs.org.au/insightsandpublications/reports-publications/digital-pulse2022.html.
8. ACSCa n.d., *Glossary - I*, Australian Cyber Security Centre, viewed 27 March 2023, https://www.cyber.gov.au/acsc/view-all-content/glossary/i.
9. ACSCb n.d., Glossary – C, Australian Cyber Security Centre, viewed 27 March 2023, https://www.cyber.gov.au/acsc/view-all-content/glossary/c.
10. Bagchi-Sen, S, Rao, HR, Upadhyaya, SJ & Chai, S 2010, 'Women in Cybersecurity: A Study of Career Advancement', *IT Professional,* 12(1), 24–31.
11. Begeny, CT, Ryan, MK, Moss-Racusin, CA & Ravetz, G 2020, 'In some professions, women have become well represented, yet gender bias persists - perpetuated by those who think it is not happening', *Science Advances,* 6(26): eaba7814.
12. Bohnet, I 2016, *What Works: Gender Equality By Design,* Cambridge, Massachusetts: Harvard University Press.
13. Buengeler, C, Leroy, H & De Stobbeleir, K, 2018, 'How leaders shape the impact of HR's diversity practices on employee inclusion', *Human Resource Management Review,* 28, 289–303.
14. Carlana, M 2019, 'Implicit stereotypes: Evidence from teachers' gender bias', *The Quarterly Journal of Economics,* 134(3): 1163-1224.
15. Cheryan, S, Master, A & Meltzoff, AN 2022, 'There are too few women in computer science and engineering', *Scientific American,* 27 July 2022, https://www.scientificamerican.com/article/there-are-too-few-women-in-computer-science-and-engineering/.
16. Cheryan, S, Plaut, VC, Handron, C & Hudson, L 2013, 'The Stereotypical Computer Scientist: Gendered Media Representations as a Barrier to Inclusion for Women', *Sex Roles,* 69(1-2), 58–71.
17. Cullen, ZB & Perez-Truglia, R 2022, 'Old Boys' Club: Schmoozing and the Gender Gap' Working Paper No. 26530, National Bureau of Economic Research, Cambridge, Massachusetts. https://www.nber.org/papers/w26530.\
18. De Gioannis, E, Pasin, GL & Squazzoni, F 2023, 'Empowering women in STEM: a scoping review of interventions with role models', *International Journal of Science Education,* Part B, DOI: 10.1080/21548455.2022.2162832.
19. Department of the Prime Minister and Cabinet, UNSW Public Service Research Group and UNSW Australian Centre for Cyber Security 2017, *Women in Cyber Security Literature Review,* Women in Cyber Security Careers Project, Canberra.
20. Dobbin, F & Kalev, A 2022, *Getting to Diversity: What Works and What Doesn't,* Cambridge, Massachusetts: Harvard University Press, US.
21. Dockery, AM & Bawa, S 2019, 'Labour market implications of promoting women's participation in STEM in Australia, *Australian Journal of Labour Economics,* 21(2): 125 – 151.
22. Fine, C, Sojo, V & Lawford-Smith, H 2020, 'Why Does Workplace Gender Diversity Matter? Justice, Organizational Benefits, and Policy', *Social Issues and Policy Review,* 14(1), 36-72, DOI: 10.1111/sipr.12064.
23. Fox, C 2017, *Stop Fixing Women: Why building fairer workplaces is everybody's business,* Sydney: New South Publishing.
24. Frost & Sullivan 2017, *The 2017 Global Information Security Workforce Study: Women in Cybersecurity.* A Frost & Sullivan White Paper, https://media.bizj.us/view/img/10398134/womenin-cybersecurity-march-2017.pdf.
25. Gergis, D & Kachala, M 2021, 'Two Ways to Improve Gender Balance in Tech', *Harvard Business Review,* https://hbr.org/2021/12/two-ways-to-improve-gender-balance-in-tech.
26. Handley, IM, Brown, ER, Moss-Racusin, CA & Smith, JL 2015, 'Quality of evidence revealing subtle gender biases in science is in the eye of the beholder', *PNAS,* 112 (43): 13201-13206.
27. Heilman, ME 2012, 'Gender stereotypes and their effects in the workplace: perceptions, reactions, and impact', *Handbook of gender research in psychology,* 2, 369-397.
28. Heilman, ME & Caleo, S 2018, 'Combatting gender discrimination: A lack of fit framework', *Group Processes & Intergroup Relations,* 21, 725–744.
29. Henn, S 2014, 'When Women Stopped Coding',

30. Hewlett, SA, Marshall, M & Sherbin, L 2013, 'How Diversity Can Drive Innovation', *Harvard Business Review,* https://hbr.org/2013/12/how-diversity-can-drive-innovation.

31. Human Resource Management International Digest 2019, 'Strengthening the call for top-down gender diversity: Exploring the relationship between productivity and gender diversity in top management teams', *Human Resource Management International Digest,* Vol. 27 No. 7, pp. 35-37, https://doi.org/10.1108/HRMID-07-2019-0187.

32. International Information System Security Certification Consortium 2018, *ISC² Cybersecurity Workforce Study,* (ISC)²: https://www.isc2.org/research/cybersecurity-workforce-study, viewed 2 February 2023.

33. International Information System Security Certification Consortium 2020, *(ISC)² Workforce Study 2020,* International Information System Security Certification Consortium.

34. (ISC)2 2022, CISSP – The World's Premier Cybersecurity Certification, (ISC)², viewed 31 January 2023, https://www.isc2.org/Certifications/CISSP.

35. Johnson, SK & Kirk, JF 2020, 'Research: To reduce gender bias, anonymize job applications', *Harvard Business Review,* March 2020.

36. Kaiser, CR, Major, B, Jurcevic, I, Dover, TL, Brady, LM & Shapiro, JR 2013, 'Presumed fair: Ironic effects of organizational diversity structures', *Journal of Personality and Social Psychology,* 104, 504–519.

37. Klambauer, G, Unterthiner, T, Mayr, A & Hochreiter, S 2017, *Self-Normalizing Neural Networks,* arXiv preprint arXiv:1706.02515, https://arxiv.org/abs/1706.02515.

38. Landreth Grau, S & Zotos, YC 2016, 'Gender stereotypes in advertising: a review of current research', *International Journal of Advertising,* 35:5, 761-770, DOI: 10.1080/02650487.2016.1203556.

39. Lapan, JC & Smith, KN 2022, 'No Girls on the Software Team: Internship Experiences of Women in Computer Science', *Journal of career development,* 0(0), 1-16: 89484532110708.

40. Lee, HW & Kim, E 2020, 'Workforce diversity and firm performance: Relational coordination as a mediator and structural empowerment and multisource feedback as moderators', *Human Resource Management,* 59(1), 5-23.

41. Lloyd, A, Gore, J, Holmes, K, Smith, M & Fray, L 2018, 'Parental Influences on Those Seeking a Career in STEM: The Primacy of Gender', *International Journal of Gender, Science and Technology,* 10(2), 308–328, Retrieved from https://genderandset.open.ac.uk/index.php/genderandset/article/view/510.

42. Margolis, J & Fisher, A 2003, *Unlocking the Clubhouse: Women in Computing,* The MIT Press.

43. Master, A, Cheryan, S, Meltzoff, AN & Graham, S 2016, 'Computing Whether She Belongs: Stereotypes Undermine Girls' Interest and Sense of Belonging in Computer Science', *Journal of Educational Psychology,* 2016, Vol.108(3), pp.424-437.

44. McKinsey & Company 2018, *Delivering through diversity,* viewed 1 February 2023,https://www.mckinsey.com/business-functions/organization/our-insights/delivering-through-diversity.

45. McKinsey & Company 2018a, *Women in the Workplace 2018,* https://womenintheworkplace.com/.

46. Michell, D, Szorenyi, A, Falkner, K & Szabo, C 2017, 'Broadening participation not border protection: how universities can support women in computer science', *Journal of Higher Education Policy and Management,* 39:4, 406 422, DOI: 10.1080/1360080X.2017.1330821.

47. Miller, T & Del Carmen Triana, M 2009, 'Demographic diversity in the boardroom: Mediators of the board-diversity - firm performance relationship', *Journal of Management Studies,* 46, 755-786.

48. National Academies of Sciences, Engineering, and Medicine; Policy and Global Affairs; Committee on Women in Science, Engineering, and Medicine; Committee on the Impacts of Sexual Harassment in Academia 2018, *Sexual Harassment of Women: Climate, Culture, and Consequences in Academic Sciences, Engineering, and Medicine,* Johnson, PA; Widnall, SE & Benya, FF (Eds), Washington, D.C: National Academies Press.

49. Ng, E & Rumens, N 2017, 'Diversity and inclusion for LGBT workers: current issues and new horizons for research', *Canadian Journal of Administrative Sciences,* 34 (2), 109-120.

50. Post, C & Byron, K 2015, 'Women on boards and firm financial performance: A meta-analysis', *Academy of Management Journal,* 58, 1546–1571.

51. Richard, OC 2000, 'Racial diversity, business strategy, and firm performance: A resource-based view', *Academy of Management Journal,* 43, 164–177.

52. Ridgeway, CL 2011, *Framed by gender: how gender inequality persists in the modern world,* Oxford University Press.

53. Risse, L 2020, 'Leaning in: Is higher confidence the key to women's career advancement?', *Australian Journal of Labour Economics,* 23(1), 43–78.

54. Rock, D & Grant, H 2016, 'Why Diverse Teams Are Smarter', *Harvard Business Review,* https://hbr.org/2016/11/why-diverse-teams-are-smarter.

55. Rønsen, M & van der Meer, T 2017, 'The gender pay gap in the OECD countries', *Oxford Review of Economic Policy,* 33(4), 642–664, https://doi.org/10.1093/oxrep/grx027.

56. Ruiz-Jiménez, JM & del Mar Fuentes-Fuentes, M 2016, 'Management Capabilities, Innovation, and Gender Diversity in the Top Management Team: An Empirical Analysis in Technology-Based SMEs', *Business Research Quarterly,* 19.2 (2016): 107–121.

57. Saffie-Robertson, MC 2020, 'It's Not You, It's Me: An Exploration of Mentoring Experiences for Women in STEM', *Sex Roles,* 83(9-10), 566–579, DOI: https://doi.org/10.1007/s11199-020-01129-x.

58. Saxena, M, Geiselman, TA & Zhang, S 2019, 'Workplace incivility against women in stem: Insights and best practices', *Business Horizons,* 62(5), 589–594.

59. Science and Technology Australia 2019, 'Sexual harassment a significant issue for STEM sector', Media Release, 1 March 2019, https://scienceandtechnologyaustralia.org.au/sexual-harassment-a-significant-issue-for-stem-sector/.

60. Sobieraj, S 2018, '"Bitch, Slut, Skank, Cunt: Patterned Resistance to Women's Visibility in Digital Publics', *Information, Communication & Society,* 21(11), 1700–1714.

61. Solms, R, & Niekerk, J 2013, 'From information security to cyber security', *Computers and Security,* 97-102.

62. Tokbaeva, D & Achtenhagen, L 2021, 'Career resilience of female professionals in the male-dominated IT industry in Sweden: toward a process perspective', *Gender, Work and Organization,* 1-40.

63. Torres-Ramos S, Fajardo-Robledo NS, Pérez-Carrillo LA, et al. 2021, 'Mentors as Female Role Models in STEM Disciplines and Their Benefits', *Sustainability,* 13(23), MDPI AG: 12938, DOI: 10.3390/su132312938.

64. Turban, S, Wu, D & Zhang, LT 2019, 'When Gender Diversity Makes Firms More Productive', *Harvard Business Review,* https://hbr.org/2019/02/research-when-gender-diversity-makes-firms-more-productive.

65. Vinkenburg, CJ 2017, 'Engaging gatekeepers, optimizing decision making, and mitigating bias: Design specifications for systemic diversity interventions', *Journal of Applied Behavioral Science,* 53, 212–234.

66. Williamson S, Creagh A & Tranter M 2017, Women in Cyber Security Literature Review, Department of Premier & Cabinet Australia.

Connect with us

By email

ccsri@rmit.edu.au

Website

rmit.edu.au/cyber

RMIT UNIVERSITY

Centre for Cyber Security Research and Innovation