POLICY PAPER

Investigating the Reasons why Women Leave the Cyber Security Workforce and Strategies to Address this Attrition

Prepared for:

awsn
Australian Women in Security Network

RMIT UNIVERSITY Centre for Organisations and Social Change

RMIT UNIVERSITY Centre for Cyber Security Research and Innovation

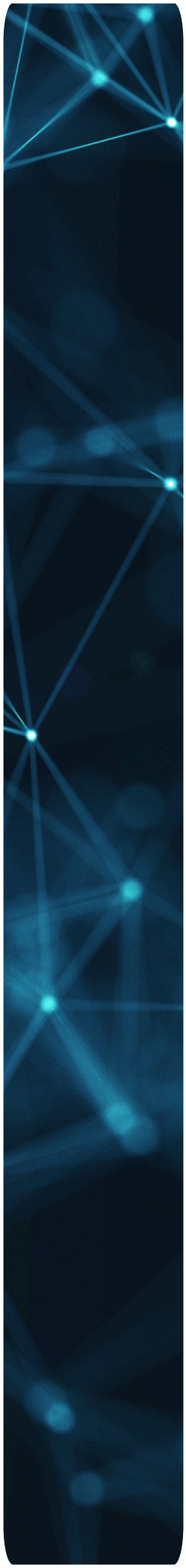
ACKNOWLEDGEMENTS

This research report was commissioned by Australian Women in Security Network (AWSN) and undertaken by RMIT University's Centre for Cyber Security Research and Innovation (CCSRI) and Centre for Organisations and Social Change (COSC). AWSN's involvement has been facilitated through sponsorship support by the Australian Signals Directorate (ASD), one of Australia's peak national security agencies.

This Policy Paper synthesises three reports: a Literature Review, Interview Findings, and the Gender Dimensions of the Australian Cyber Security Sector Report (Phase I of this study). The RMIT research team includes Assoc. Prof Lena Wang, Assoc. Prof Lauren Gurrieri, Dr Bronwyn Bruce, Karthika Kumar, Salvatore Ferraro, Dr Amy Corman, Prof Matthew Warren, Amal Varghese, Gabriela Cincotta and Lee-ann Phillips.

The RMIT research team thanks Jacqui Loustau and the team at AWSN for their support in the development of this report. This report uses data collected from various sources and all data is used with permission. The authors thank all participants for sharing their experiences by undertaking interviews. The findings and views presented in this report were produced independently and are those of the authors only.

TABLE OF CONTENTS



1. EXECUTIVE SUMMARY

Australian Women in Security Network (AWSN) commissioned RMIT University's Centre for Cyber Security Research and Innovation (CCSRI) and Centre for Organisations and Social Change (COSC) to undertake Phase II of a research study investigating the reasons why women are under-represented in Australia's cyber security workforce and why the few that do enter the sector, leave the sector.

Phase II builds on key findings from Phase I of this study: women only account for 17 per cent of the cyber security workforce in Australia (Risse et al., 2023). This is a sign of gender inequity. Women's low level of participation in the cyber security workforce demonstrates the influence of gender biases, stereotypes and inequities that prevail across the sector. 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. There is a growing consensus that the profession needs to broaden the diversity of its workforce to address the global shortage of cyber security professionals, including targeting recruitment and retention initiatives to women and people from disadvantaged communities (OECD, 2023).

This study's aim is to help boost the number of women entering, and staying in, the cyber security sector.

The research study comprised three parts:

1. A literature review – that builds on Phase I of this study – of gendered barriers and enablers in the cyber security workforce.
2. In-depth interviews with 30 women working in cyber security roles with over five years of experience, or those who have recently left the sector.
3. Thematic analyses of the interviews of women working in cyber security roles.

This study found that there are significant gendered barriers that contribute to the low level of recruitment to, and retention of women in, the cyber security sector. These can be attributed to cultural factors, societal attitudes, organisational barriers, the nature of jobs in the industry, and a lack of interest from women to enter the cyber security workforce.

This report makes 14 recommendations to boost the recruitment and retention of women in the cyber security workforce.

2. OBJECTIVES AND CONTEXT

The research objectives of Phase II of this study (Investigating the Reasons why Women Leave the Cyber Security Workforce and Strategies to Address this Attrition) were to:

- Identify gendered barriers and enablers to improving the recruitment and retention of women in the cyber security profession, and their cultural and institutional context.
- Develop a deep understanding of the reasons women leave the cyber security profession.
- Gain insights into the lived experiences of women in the cyber security sector, focusing on challenges and opportunities for improvement.
- Identify how these issues can be addressed by employers, industry groups and governments.
- Explore the potential interventions and strategies for organisations to implement to enhance gender diversity and retention of women in the cyber security workforce.

3. RECOMMENDATIONS

To make Australia's cyber security workforce more gender-balanced and inclusive, a whole-of-society approach is needed. This includes employers, leaders, government, schools, media, and the community. They all need to change their policies, practices, and attitudes about gender equality.

To improve gender equality in cyber security, we should use methods that are proven to work. Research shows that instead of expecting women to adapt to unfair systems, we need to change the systems, cultures, and traditions themselves.

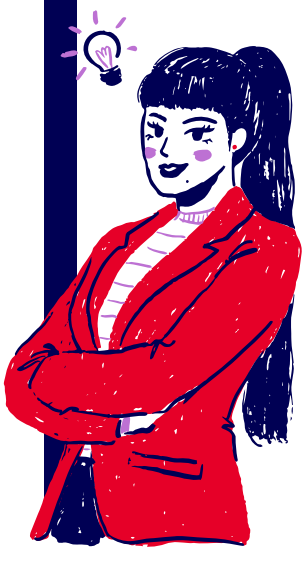
Based on RMIT’s research and interviews, this report outlines practical steps that different players in the ecosystem can take to improve gender equality and inclusion in Australia’s cyber security sector. These recommendations apply to society as a whole, organisations, and the entire profession.

3.1 Societal and profession-wide initiatives designed to improve recruitment and retention of women

The table below presents societal and profession-wide recommendations for government and industry peak bodies to boost the recruitment, and retention, of women in the cyber security profession in Australia.

Table 1: *Societal and profession-wide recommendations to improve recruitment and retention of women in cyber security*

Recommendation 1: Government and industry bodies should invest in unconscious bias and gender inclusive training programs
• Participants noted that a **male-dominated culture leads to behaviours that exclude women**, leaving them feeling unwelcome in cyber security. • To tackle the **problem of low recruitment of women** in cyber security, we recommend that government and industry organisations invest in training programs that focus on unconscious bias and gender inclusivity. They should highlight the specific challenges and barriers that women encounter in the cyber security field.
Recommendation 2: Government and industry bodies should promote women's interest in the cyber security profession
• Female cyber security professionals RMIT interviewed shared compelling reasons for choosing and staying in their career, such as their ability to safeguard their community through their job. **To attract more women to the field**, industry leaders and governments should promote the profession's positive social impact. This will inspire more women to consider cyber security as a career path.
Recommendation 3: Implement educational programs as early as possible
• The evidence suggests that **women are not typically interested in a career in cyber security, and STEM fields more broadly**. To spark girls' interest in cyber security, educational programs should begin as early as primary school and continue into secondary school.



Recommendation 4: Collect longitudinal data regarding efficacy of educational programs

- Many programs aimed at increasing women's involvement in cyber security (and STEM fields) start with girls in primary and secondary schools. These initiatives need time to show results, and **there is not yet have enough data to know how well existing educational programs are working.** To make smart decisions about what really works, we need to gather information over a longer period. This could be done through a specific long-term study or by adding new questions to existing surveys like the national Census.

Recommendation 5: Government and industry peak bodies should support closing the gender pay gap

- Government and industry leaders should offer clear guidance to organisations on how to **carry out internal audits of the gender pay gap**. They should provide advice on how to ensure that women in cyber security roles receive fair pay and benefits.

Recommendation 6: Establish/expand women's networks

- Establish and/or expand women's networks **to encourage a sense of female community; this may foster confidence and enjoyment** for women in the sector.
- Industry bodies should help organisations co-ordinate mentoring and allyship programs.

Recommendation 7: Collect and publish data on cyber security sector gender equality indicators

- There is **inadequate data, especially at an organisation level, on the number of women entering and remaining in cyber security**. Government agencies and industry leaders should gather and publish data on gender equality and retention rates in the cyber security profession every year. This **transparency will help organisations and governments measure progress** against these indicators.

3.2 Workplace practices and conditions designed to improve recruitment and retention of women

The following are organisational level recommendations relating to workplace practices and conditions designed to boost recruitment of women into the cyber security profession in Australia.

Table 2: *Organisational level recommendations to improve recruitment and retention of women in cyber security*

Recommendation 8: Review organisational policies
• Review existing organisational policies to **ensure policies are gender neutral and target improving the workplace culture and organisational practices**.
Recommendation 9: Implement gender neutral recruitment practices
• Revise organisational recruitment practices and processes to **reduce unconscious bias and create a fairer hiring environment** – this includes anonymised resumes/CV screening, skills forms, diverse hiring panels, and other gender-neutral recruitment practices that can improve the recruitment of women to cyber security roles, including senior managerial roles.
Recommendation 10: Design and redesign jobs to appeal to and accommodate women
• Organisations can do more to attract, support and keep women in cyber security, especially those with caring responsibilities or who want to work part-time. This can be achieved by: redesigning jobs to move away from a 24/7 work culture, where practical; offering more flexible work arrangements; and, creating cyber security roles that are suitable for part-time work or job-sharing. These changes would greatly benefit women and help organisations retain valuable talent.

Recommendation 11: Implement formal mentoring and allyship programs

- To **help women advance in their cyber security careers**, organisations and industry leaders should set up formal mentoring programs specifically for women; and companies should consider creating allyship programs. This will **improve gender inclusion across the organisations and build supportive relationships with underrepresented groups**, including women and other diverse groups.

Recommendation 12: Enhance professional development opportunities for women

- Encourage women in cyber security to pursue professional development opportunities, particularly cyber security skills or management and leadership. These opportunities could be partially subsidised by the organisation, industry peak bodies and/or government to **mitigate the cultural and institutional barriers to women's career advancement in the profession**.
- Implement women-only training programs (WOTPs) to **support career advancement for women in the workforce.** These programs can: **boost women's career progression; increase their confidence and self-belief; enhance their leadership skills;** and **help clarify personal and professional goals**.

Recommendation 13: Industry bodies could implement programs to support women to re-enter the cyber security workforce

- Design and roll out programs to **support women returning to the cybersecurity workforce.** The programs should: target women re-entering after career breaks or changing fields; focus on roles at various career levels, including mid and senior positions; leverage transferable management skills from other industries; identify and address education gaps for successful re-entry. Industry organisations could lead such initiatives to **strengthen the cybersecurity talent pool and promote gender diversity**.

Recommendation 14: Report on equality indicators

- Increase disclosure of gender equality indicators to **deliver meaningful organisational-level change**.

4. SUMMARY OF KEY FINDINGS

Table 3: *Summary of key findings from the Phase II literature review*

Australia's cyber security workforce
• The cybersecurity industry in Australia faces a significant gender imbalance, with women underrepresented in the workforce. This issue remains poorly understood due to a lack of comprehensive data and research. The field is predominantly male, which creates barriers for women entering and staying in cybersecurity careers. These barriers include: persistent gender stereotypes • A masculine-oriented work culture; discouragement for women to pursue or maintain careers in the sector. This gender disparity limits the diversity of talent and perspectives in the cyber security workforce, and potentially impacting Australia's ability to address evolving security challenges effectively.
Gender inequality statistics in cyber security and STEM disciplines internationally
• Women account for less than one in five cyber security professionals, according to empirical evidence. This low female representation extends to leadership positions. • Gendered workplace segregation is present in STEM occupations; Cyber security is no exception. Women are over-represented in administrative and clerical roles, which are lowly paid compared to technical and managerial roles. This may be the reason for the sizeable gender pay gap (between 12 and 25 per cent from the evidence), in Australia, in cyber security and related STEM occupations.
Promoting gender diversity and inclusion in the cyber security profession
• There is a need to expand and spread successful programs that help more women join the cyber security field. To do this, organisations should: set clear goals for hiring women and openly share progress on gender equality; change how cyber security jobs are designed; move away from expecting constant availability and long hours; create a workplace culture that welcomes women; and, provide clear paths for women to advance in their careers. These steps can help reduce the current gender imbalance in cyber security. By taking action, we can build a stronger, more diverse workforce.

Table 4: *Summary of key findings from interviews of women working in the cyber security profession*

Gendered barriers in cyber security in Australia
• Participants noted that **gender equity is an ongoing struggle** in the cyber security industry. Whilst there have been some advances, with the representation of women increasing in recent years, the pace of change was characterised as unsatisfactory overall, with true equality yet to be achieved. • The cyber security industry faces significant challenges due to gender imbalance, in terms of: the work environment; the industry being predominantly male and women feeling pressure to adapt to this environment. Women reported commonly experiencing professional disrespect, bullying, harrassment and discrimination. There's a clear need for a more inclusive and supportive atmosphere to ensure women have a positive workplace experience. • Participants highlighted that from a gender pay equity perspective, they believed they were not equally paid compared to their male colleagues. • In terms of age and representation, female cyber professionals tend to be younger than their male counterparts. This suggests that there is a growing representation of women through generational change, however there exists potential barriers for older women who want to enter the sector. • Cyber security roles are highly demanding (and can include a 24/7 culture for operational role); they are typically not compatible with achieving work-life balance. This makes it difficult, especially for women in senior leadership positions and/or those with domestic and/or family responsibilities. Limited organisational support offered to women returning from maternity leave was also highlighted. • Participants noted that they have experienced doubts around their self-efficacy which have arisen from cyber security being a male-dominated field. Participants also noted that women lacked interest in cyber security, which stems, in part, from gendered stereotypes that start at an early age.

Enablers to reduce gender inequity in cyber security in Australia

- Participants were ambivalent about implementing explicit gender targets due to concerns that their own competence, as well as those of the women hired to fulfil a gender target, would be questioned.
- Flexible work arrangements were viewed favourably, with suggestions that managers could be more open-minded and flexible with job design to accommodate experienced women seeking to work part-time in cyber security. This includes work from home arrangements and part-time roles.
- Participants stated that they had benefited from mentoring programs, especially those with male sponsors. And they highlighted the benefit of professional development (PD) programs, especially managerial and leadership skills PD programs, which are important for career progression.
- Several participants agreed that promoting interest in cyber security among school-aged girls was necessary to challenge gendered stereotypes that arise at an early age.

5. METHODOLOGY AND DATA

The methodology for the research study was:

1. A literature review of gendered barriers and enablers in the cyber security workforce (building on the literature review undertaken in Phase I of the study);
2. In-depth interviews with 30 women with over five years of experience working in cyber security roles, who are either currently working in the cyber security workforce, or who have recently left the cyber security workforce; and
3. Thematic analysis of the interviews of the women who are working in, or have recently worked in, cyber security roles.

Details of this methodology and the data collected are provided below.

5.1 Phase II Literature Review

Building on the literature review completed in Phase I, the Phase II literature review focused on an in-depth review of more up-to-date literature that explored two key areas:

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

5.2 Qualitative Interviews and Thematic Analysis

Qualitative interviews

Interviews were conducted with 30 female participants who had at least five years of experience working in cyber security, and all of whom are currently or previously employed in the cyber security workforce. Their participation was voluntary, with most participants being members of the Australian Women in Security Network (AWSN).

Each participant responded to an invitation email to participate that was disseminated by AWSN, and the participants were not paid to be interviewed. The interviews were conducted via Microsoft Teams between late April and early July 2024, with the average interview duration being 48 minutes.

Identifying information about the participants is not disclosed in this report. As such, participants in the report were assigned a randomised identification number.

The qualitative interviews offer insights into the lived experiences of participants, including:

- The motivations for entering the cyber security profession, whether they have considered leaving the profession, and what aspects of their role they value most.
- The gendered barriers they have confronted in the early, middle and more advanced stages of their career.
- How they have sought to navigate those gendered barriers, and
- The extent to which their career advancement has benefited from the implementation of organisational policies and practices designed to improve gender diversity and inclusion.

These insights can enable organisations and the sector as a whole to devise better policies and practices that attract and retain high calibre women cyber professionals.

Thematic Analysis of Interview Data

Thematic analysis represents a method of identifying patterns and recurring themes that are present in qualitative data collected from interview participants (Braun & Clarke, 2006). NVivo qualitative data analysis software was used to analyse interview transcripts, where nodes reflect themes that correspond to gendered barriers and disparities evident in the cyber security profession.

In this report, the selection and structure of themes were guided by the literature review and through an inductive approach, where common responses from interview participants also shaped the selection and structure of themes (Braun & Clarke, 2006).

6. REFERENCES

Acker, J. (1990). Hierarchies, jobs, bodies: A theory of gendered organisations. Gender & society, 4(2), 139-158.

Ahuja, M. (2002). Women in the Information Technology Profession: A Literature Review, Synthesis and Research Agenda. European Journal of Information Systems, 11, 20-34. https://doi.org/10.1057/palgrave/ejis/3000417.

Aljuaid, A. (2022). Empowering Women in Saudi Arabia to Access Cybersecurity Opportunities: A Qualitative Study. ProQuest Dissertations Publishing].
Australian Department of Home Affairs. (2023). 2023-2030 Australian Cyber Security Strategy. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). Women in Cybersecurity: A Study of Career Advancement. IT professional, 12(1), 24-31. https://doi.org/10.1109/MITP.2010.39

Betz, N.E. (2004). Contributions of Self-Efficacy Theory to Career Counseling: A Personal Perspective. The Career development quarterly, 52(4), 340-353. https://doi.org/10.1002/j.2161-0045.2004.tb00950.x

Bilal, M., Balzora, S., Pochapin, M. B., & Oxentenko, A. S. (2021). The Need for Allyship in Achieving Gender Equity in Gastroenterology. The American journal of gastroenterology, 116(12), 2321-2323. https://doi.org/10.14309/ajg.0000000000001508

Bongiovanni, I., & Gale, M. (2023). Women in Cyber: Exploring the Barriers, Redesigning the Profession. https://business.uq.edu.au/files/97978/women-in-cyber-exploring-the-barriers-report.pdf

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Chasserio, S., & Bacha, E. (2024). Women-only training programmes as tools for professional development: analysis and outcomes of a transformative learning process. European Journal of Training and Development, 48(3/4), 455-477.

Crumpler, W., & Lewis, J.A. (2022). Cybersecurity Workforce Gap. JSTOR. https://www.jstor.org/stable/pdf/resrep22540.pdf

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in ‘real world’ policing and law enforcement. The Police Journal, 96(4), 573-592. https://doi.org/10.1177/0032258x221107584.

Da Silva, J., & Jensen, R. B. (2022). " Cyber security is a dark art": The CISO as Soothsayer. Proceedings of the ACM on Human-Computer Interaction, 6(CSCW2), 1-31.

Das, S., & Jha, S. (2024). Women’s career advancement: review of literature and future research agenda. Humanomics, 40(2), 232-255. https://doi.org/10.1108/IJOES-12-2022-0313

DeCrosta, J. (2021). Bridging the Gap: An Exploration of the Quantitative and Qualitative Factors Influencing the Cybersecurity Workforce Shortage ProQuest Dissertations Publishing].

Del Toro, E. (2019). Introducing Women to Computer Science in High School to Reduce the Gender Gap in the Cybersecurity Profession ProQuest Dissertations Publishing].

Drury, B. J., Siy, J. O., & Cheryan, S. (2011). When do female role models benefit women? The importance of differentiating recruitment from retention in STEM. Psychological Inquiry, 22(4), 265-269.

Fitzsimmons, T. W., Yates, M. S., & Callan, V. J. (2020). Employer of Choice for Gender Equality: Leading practices in strategy, policy and implementation. Brisbane: AIBE Centre for Gender Equality in the Workplace.

Foley, M., Dewey, L., Williamson, S., Blackman, D., Creagh, A., Davidson, L., Zhu, M., & Slay, J. (2017). Women in cyber security literature review.

Garg, S., & Sangwan, S. (2021). Literature Review on Diversity and Inclusion at Workplace, 2010–2017. Vision, 25(1), 12-22. https://doi.org/10.1177/0972262920959523

Ghalebeigi, A., Gekara, V., Douglas, K., Ferraro, S., Wang, L., & Safari, M. (2022). Assessing Progress in Implementing the Gender Equality Act 2020.

Giboney, J.S., Anderson, B.B., Wright, G.A., Oh, S., Taylor, Q., Warren, M., & Johnson, K. (2023). Barriers to a cybersecurity career: Analysis across career stage and gender. Computers & security, 132, 103316. https://doi.org/10.1016/j.cose.2023.103316

Givens, E. W. (2019). Perception versus Reality: The Perceived Cybersecurity Workforce Shortage in the United States Capitol Technology University].

Goldin, C. (2014). A grand gender convergence: Its last chapter. American economic review, 104(4), 1091-1119.

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

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

Hartman, R.L., & Barber, E.G. (2020). Women in the workforce: The effect of gender on occupational self-efficacy, work engagement and career aspirations. Gender in management, 35(1), 92-118. https://doi.org/10.1108/GM-04-2019-0062

Hideg, I., & Krstic, A. (2021). The quest for workplace gender equality in the 21st century: Where do we stand and how can we continue to make strides? Canadian Journal of Behavioural Science/Revue canadienne des sciences du comportement, 53(2), 106.

Hinojosa, T., Rapaport, A., Jaciw, A., & Zacamy, J. (2016). Exploring the Foundations of the Future STEM Workforce: K-12 Indicators of Postsecondary STEM Success. REL 2016-122. Regional Educational Laboratory Southwest.
ISC2. (2018). Women in cybersecurity. www.isc2.org/-/media/ISC2/ Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx

ISC2. (2023). How the economy, skills gap and artificial intelligence are challenging the global cybersecurity workforce. https://www.isc2.org/Research/Economy-Skills-Gap-AI-Cybersecurity-Workforce.
ISC2. (2024). Women in cyber security: Inclusion, advancement and pay equity are keys to attracting and retaining more women.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Professionals Australia (2017). Gender Segregation in the STEM Professions.

Radu, C. & Smaili, N. (2022) Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Related Disclosure. Journal of Business Ethics, 177, 351–374 (2022). https://doi.org/10.1007/s10551-020-04717-9.

Raytheon. (2017). Securing Our Future: Cybersecurity and the Millenial Workforce.

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

Risse, L., Beamond, M., Hall, J., Wang, Y., Warren, M., Barua, B., & Kondylas, L. (2023). Gender Dimensions of the Australian Cyber Security Sector. https://www.rmit.edu.au/content/dam/rmit/au/en/research/networks-centres-groups/centre-for-cyber-security/gender-dimensions-of-the-australian-cyber-security-sector-report.pdf

Rowland, P., & Noteboom, C. (2019). Influencing the Future: Adolescent Girls' Perceptions of Cybersecurity Careers.

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

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

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

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

RMIT UNIVERSITY Centre for Organisations and Social Change

RMIT UNIVERSITY Centre for Cyber Security Research and Innovation