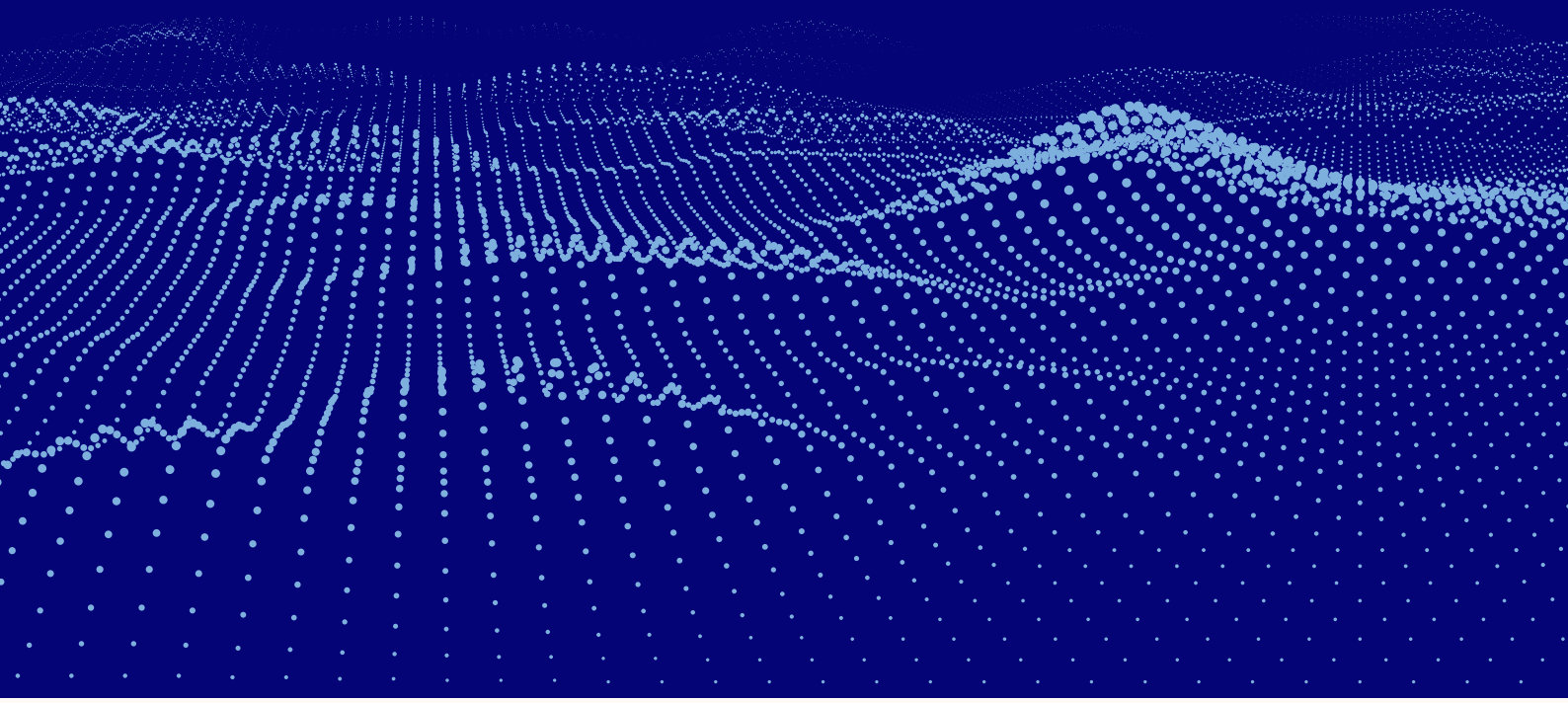
Decoding cyber security

Meeting national workforce needs and improving gender equity

May 2026



Cyber5050

CyberCX Part of Accenture

FW

awsn Australian Women in Security Network

CIT Canberra Institute of Technology

Australian Services Union By your side

Liu, P. M., A. Edwards, R. Ismail, R. Leahy Gatfield, J. Loustau and B. Kendrick (May 2026) Decoding Cyber Security: Growing an inclusive workforce. Report by FW and the Australian Women in Security Network for the Cyber5050 Partnership, funded by the Commonwealth of Australia. www.futurewomen.com/cyber5050/decoding-cyber-report

FW is dedicated to gender equity in Australia and supports organisations to build fair and inclusive workplaces.

The Australian Women in Security Network is a network of people aimed at educating women and girls on security and increasing the number of women in the security community.

Cyber5050 is a collaborative partnership between FW, CyberCX, the Australian Women in Security Network, the Australian Services Union and the Canberra Institute of Technology. The partnership is funded by the Department of Employment and Workplace Relations' Building Women's Careers Grant.

Building Women's Careers
An Australian Government Initiative

The Cyber5050 partnership was founded in 2025 to drive cultural and structural change in the cyber security industry as part of the Australian Government's Building Women's Careers Program. Together CyberCX, Future Women, the Australian Women in Security Network, the Australian Services Union and the Canberra Institute of Technology have produced this leading-edge research report.

This report, emerging out of broader research, presents diverse and specialised insights of Australia's contemporary cyber security professionals – real experiences, sometimes confronting. The recommendations proposed herein are therefore significant, inclusive and aimed at organisations to implement both immediately and over the longer term.

Increasing and sustaining women's participation in Australia's digital and technology industry is worth it. As this report observes, women represent only 17 per cent of the Australian cyber security workforce, even lower than the already low global average of 25 per cent.

I am certain this significant work provides an excellent foundation for the Cyber5050 collaboration to address the systemic barriers to women's participation across the cyber security workforce and achieve gender parity.

The Hon Andrew Giles

Minister for Skills and Training

Australia's cyber security workforce faces a crucial challenge – addressing a skills shortage at a time of enhanced cyber threats.

Part of the answer is increasing the number of women in cyber security. Despite women comprising 48 per cent of the national workforce as a whole, they remain strikingly underrepresented in cyber security, accounting for only 17 per cent of the workforce.[1]

FW supports women who work and women who want to work, including in cyber security. This research highlights the obstacles preventing women's participation, and removing these obstacles requires collective attention.

FW, in consultation with the Australian Women in Security Network, led this industry research as part of our participation in the Cyber5050 partnership. Funded through the Commonwealth Government's Building Women's Careers grant, this initiative is pioneering cultural and structural change across the Australian cyber workforce.

We gathered qualitative insights into the lived experiences and career trajectories of professionals who are working in, have worked in and want to work in cyber security in Australia. Our findings build on recent research exploring the attrition of women in cyber security and specifically explore gender-based microaggressions in the cyber workforce.

This report offers actionable steps to build a more equitable cyber security workplace. This is vital to the vision outlined in the *Australian Cyber Security Strategy 2023-2030*, which makes clear that if employers do not foster inclusive cultures, the sector will not have the talent to combat not only increasing cyber threats,[2] but also the unforeseen consequences of rapidly developing AI and quantum computing.

Australia deserves an inclusive cyber security workforce, and improving equity is one way to achieve this goal.

Helen McCabe

Founder and Managing Director, FW

[1] RMIT University (2023), p. 9.

[2] Department of Home Affairs (2023), p. 48.

The Australian Women in Security Network (AWSN) was founded in 2015 to connect women in security who often felt isolated in their workplaces or studies. As a not-for-profit association, AWSN is dedicated to empowering and increasing the representation of women and girls in security through connection, confidence, and capability.

Despite making up half the population, our academic study with RMIT in 2022, funded by the Australian Signals Directorate found that women represent only 17 per cent of the security workforce in Australia. Through events, mentorship, education, and advocacy, AWSN supports women at every stage of their journey, providing access to networks, knowledge, and opportunities to thrive.

We believe diverse perspectives are essential to tackling today's complex security challenges. Defending Australia, its people, businesses, and institutions requires inclusive thinking and a workforce that reflects the diversity of those we protect.

Over the past decade, we've seen progress, but it's not enough or changing fast enough. This report highlights persistent barriers that prevent our industry from reaching its full potential. Some testimonies and findings may be confronting, but they reflect real experiences we hear far too often in some organisations. Everyone deserves a safe, respectful workplace where they can contribute meaningfully.

To meet the demands of a rapidly evolving threat landscape, we must attract and retain diverse talent. This requires systemic change across all levels and sectors to create environments where people can enter, grow, and lead.

This report shares the voices of those in our industry, and outlines actions we can take together to build a stronger, more inclusive future in the cyber security industry.

Jacqui Loustau

Chief Executive Officer, Australian Women in Security Network

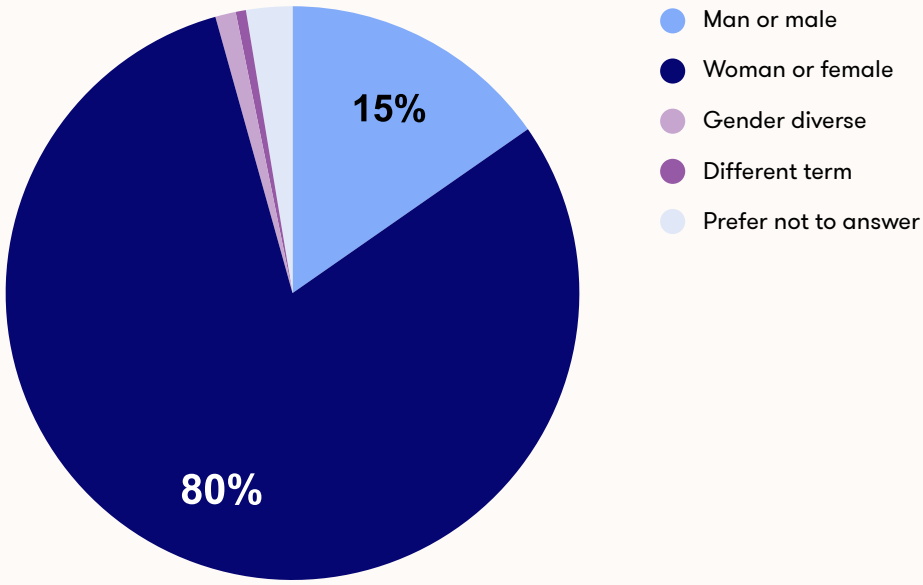
EXECUTIVE SUMMARY

Australia's cyber security workforce faces a critical skills shortage at a time of escalating cyber threats. Women represent only 17 per cent of the Australian cyber security workforce, lower than the global average of 25 per cent. Addressing barriers to women's participation, progression and retention in cyber security is essential to develop available skills and grow the workforce.

This report presents findings from a national survey of 346 respondents, as well as an in-person consultation held at the AWSN Summit in 2025. Respondents included individuals currently working in, previously working in, and aspiring to work in cyber security in Australia.

Cyber security remains a male-dominated industry, which means individual teams and workplaces are more often than not, male-dominated too. This continues to limit women engaging with the industry, with 89 per cent of respondents agreeing that most people working in cyber security are men. Gender bias in recruitment creates a serious barrier, manifesting as unconscious affinity bias, an over-emphasis on technical skills and work experience, and career break stigma. Despite the demand for skilled workers, there are limited pathways to enter cyber security. Women were more likely to enter through a referral from a network or a graduate program, while men were more likely to enter by transitioning from the same organisation or industry, a job search platform, or industry programs. The lack of available part-time opportunities also prevented mothers and carers from entering or returning to the workforce.

Figure 1. Gender breakdown of survey respondents



Women reported feeling less respected and less able to contribute meaningfully at work than men, and are less likely to feel a sense of belonging. They are significantly more likely than men to experience gender-based microaggressions, including assumptions about their emotional sensitivity, inappropriate comments about their appearance, and being excluded from decision-making or leadership opportunities. Only 21 per cent of respondents reported microaggressions, suggesting the unreported rate is much higher.

Women also reported experiencing bullying and sexual harassment, revealing that some workplaces are not meeting their legal responsibilities under the Respect at Work Act 2022 and Sex Discrimination Act 1984 (Cth).

The majority of cyber professionals (85%) work additional hours per week, and 72 per cent reported experiencing burnout. Only 45 per cent of women feel there is a clear progression pathway within their organisation, compared to 65 per cent of men, and only 57 per cent believe women and men have the same opportunities for promotion, compared to 82 per cent of men. Visible role models, transparent promotion and pay practices, inclusive workplace policies, and technical training were identified as the most valued supports for retention and progression.

Of those who left cyber security, the most cited reason was redundancy or termination, though a hostile working environment was also a notable factor. 40 per cent of women agreed that their gender contributed to their decision to leave. The majority of those who left did not feel supported when they departed.

This report makes recommendations for cyber security organisations and the sector, offering both immediate actions and longer term strategies.

An immediate action is to take a zero-tolerance approach to microaggressions and to bullying and sexual harassment. Other actions to be taken in the short term include addressing excessive workloads and burnout, committing to inclusive marketing and job advertisements, investing in inclusive recruitment, creating opportunities for progression, and maintaining and expanding flexible work opportunities.

Longer term actions are also required. These include committing to culture change from the top, engaging men as agents of change, reporting on gender leadership and pay gaps, and building long-term pipelines into the profession.

About this report

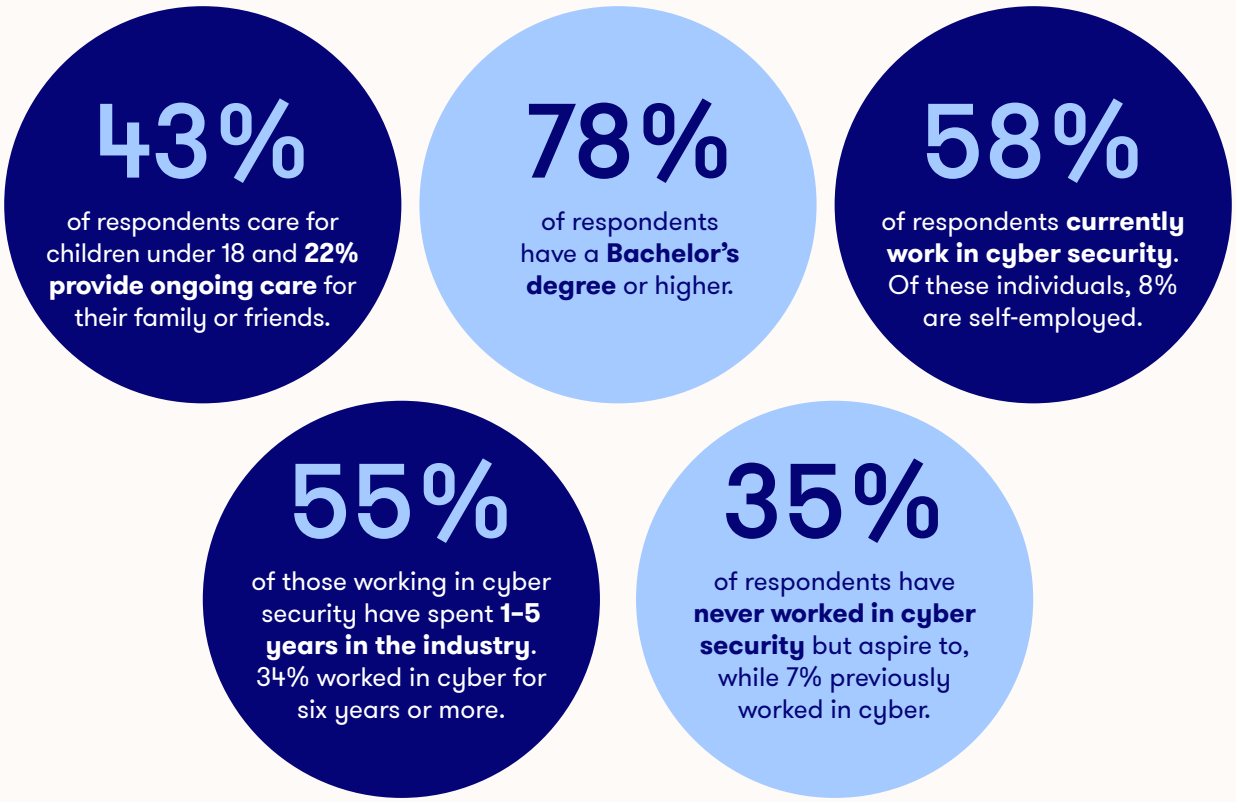
Cyber security has high barriers to entry, and women and gender diverse people are often excluded from or marginalised in the cyber workplace once they enter.

To drive cultural and structural change in the cyber security industry, in 2025 FW, CyberCX, the Australian Women in Security Network, the Australian Services Union and the Canberra Institute of Technology founded the Cyber5050 partnership. This partnership is funded until 2027 by the Australian Federal Government's Building Women's Careers Grant.

As part of the partnership, FW and the Australian Women in Security Network conducted a survey to understand the barriers to recruitment, progression and retention in cyber security in Australia. We surveyed people who are currently working in or who have previously worked in cyber security in Australia, as well as people who are trying to move into a cyber security role in Australia. We received a total of 346 responses. We also held a consultation on 1 August 2025 at the AWSN Summit.

Our findings broadly align with and build on recent research, and contribute to an understanding of the experience of microaggressions in the cyber security industry in Australia. Our recommendations provide guidance for cyber security organisations and the sector, to build inclusive workplaces and strengthen Australia's cyber security landscape.

Figure 2. Respondent demographics



The research to date

Cyber security breaches are becoming more frequent and pose greater risks to individuals and organisations.[3] At the same time the Australian workforce is experiencing a critical and ongoing skills shortage.

Compounding this is the gender divide within cyber security. Women represent only 17 per cent of the Australian cyber security workforce,[4] which sits even lower than the already low global average of 25 per cent.[5] Addressing barriers to women's participation, progression and retention in cyber security is critical, as this will expand the workforce and unlock 'vital skills, diverse thinking and new leadership potential to a rapidly evolving field'.[6]

Encouragingly, progress has been made in recent years. There was a fourfold increase in women entering specialist ICT security roles between 2016 and 2021, compared to a threefold increase for men.[7] There is also a growing number of women completing cyber security training courses, setting themselves up for technical roles.[8] Nevertheless, structural disparities persist, including the disheartening findings that women in cyber security are disproportionately represented in lower-paid administrative and clerical positions, and remain underrepresented in technical and managerial roles.[9]

Persistent gendered stereotypes and ongoing bias are significant factors driving the gender pay gap and the gendered leadership gap in cyber security.[10] This is because girls and young women are socialised to view science, technology, engineering and mathematics (STEM) as male-dominated arenas. This has a documented effect of discouraging girls from pursuing STEM pathways, which over time narrows the perceived opportunities for women seeking to enter cyber security.[11] We use the word 'perceived' deliberately here, because while not all cyber security roles are highly technical, gendered stereotypes such as the 'geeky technician' contribute to the perception that all cyber security professionals fit a narrow, male-dominated and technical-only archetype.[12]

Gender stereotypes are also deeply embedded within recruitment practices.[13] Cyber security job advertisements employ the most stereotypically masculine language of any occupation, using terms associated with leadership, analytical thinking, control, and problem-solving.[14] These advertisements require, on average, around 11 skills, compared to the eight skills typically listed in other sectors.[15] Entry-level roles that demand extensive

[3] Australian Cyber Security Centre (2022), p. 47.
[4] RMIT University (2023), p. 9.
[5] Cybersecurity Ventures (2023).
[6] Canberra Cyber Hub (2025).
[7] RMIT University (2023), p. 9.
[8] Bongiovanni and Gale (2023), p. 10.
[9] RMIT University (2024), p. 11.
[10] RMIT University (2023), p. 40.
[11] Ibid.
[12] Ibid.
[13] Department of the Prime Minister and Cabinet (2023), p. 4.
[14] Ibid.
[15] Ibid.

experience are a persistent challenge that prevents women from entering cyber security.[16] Collectively, these create a structural barrier for women, who often self-select out of applying for cyber security roles.

Once a woman enters cyber security, barriers remain. For example, only 24 per cent of women report having a role model of their own gender, compared to 51 per cent of men.[17] The importance of role models on career development across genders and at all career stages is significant.[18] The high attrition rate for women in cyber security is driven by cultural factors, which include but are not limited to long working hours, being excluded from the 'boys' club', and experiencing microaggressions, as well as the persistent stereotype that women aren't cut out for technical roles or high-pressure situations.[19] High rates of bullying and sexual harassment are also well-documented across STEM industries, including cyber security.[20] Women working in cyber security who have been subjected to such treatment report long-term consequences such as imposter syndrome and mental health challenges.[21]

Research indicates that many women exit cyber security after roughly four years, suggesting that the ongoing underrepresentation of women cannot be addressed through recruitment alone.[22] Building inclusive workplace cultures that support the retention and progression of women is critical.

Opportunities for the sector

With the unprecedented level of investment into cyber security and the widespread adoption of AI across industries,[23] there is a clear and ongoing need for skilled cyber professionals. This means there are immediate opportunities to leverage the existing and transferable skills of women and gender diverse people from other industries looking to transition into cyber security.

A critical, often overlooked opportunity for the cyber security industry lies in framing the profession as not merely technical, but as an inherently purpose-driven defence against cyber threats.[24] This emphasis is essential for recruiting and retaining younger generations, particularly as an overwhelming majority of Gen Z (89%) and Millennials (92%) cite a sense of purpose as very or somewhat important for their job satisfaction and well-being.[25]

[16] Bongiovanni and Gale (2023), p. 26.
[17] RMIT University (2023), p. 27.
[18] Ibid.
[19] Department of the Prime Minister and Cabinet (2017), p. i.
[20] RMIT University (2023), p. 18.
[21] Ibid.
[22] RMIT Centre for Cyber Security Research and Innovation (2025), p. 12.
[23] Australian Trade and Investment Commission (2025).
[24] UNSW (2025).
[25] Deloitte (2025).

As predominantly digital workplaces, cyber security organisations and teams within larger, non-cyber organisations could model industry-leading flexible work practices.[26] With the capacity to work remotely, the industry has potential to attract a workforce that is not limited by geography or caring responsibilities.

In addition, cyber security careers often come with high job security[27] and above average salaries (for example, the average weekly earnings of an ICT Security Specialist is $2,228).[28] This is attractive for individuals, of course, but it has benefits at a national level. Increasing the gender diversity of the cyber security workforce could help narrow the gender pay gap. Different from equal pay for like-for-like roles, the gender pay gap measures the difference in earnings between women and men across organisations, industries and Australia as a whole.[29]

This existing pipeline of talented women and gender diverse people is not being adequately tapped, but with the right interventions, this talent could enter the cyber workforce and contribute to safeguarding Australia's digital future.

[26] Swinburne Open Ed (2025).
[27] Department of Employment and Workplace Relations (2025).
[28] Ibid.
[29] Workplace Gender Equality Agency (2026).

1. CHALLENGES FOR THE INDUSTRY

This chapter explores the state of play in Australian cyber security workplaces and focuses on the common challenges experienced in the work environment. All data in this chapter is from respondents who currently work in or previously worked in cyber security in Australia.

We urge compassion and care when reading this chapter, as not everyone in the cyber security workforce has experienced a safe and inclusive work environment.

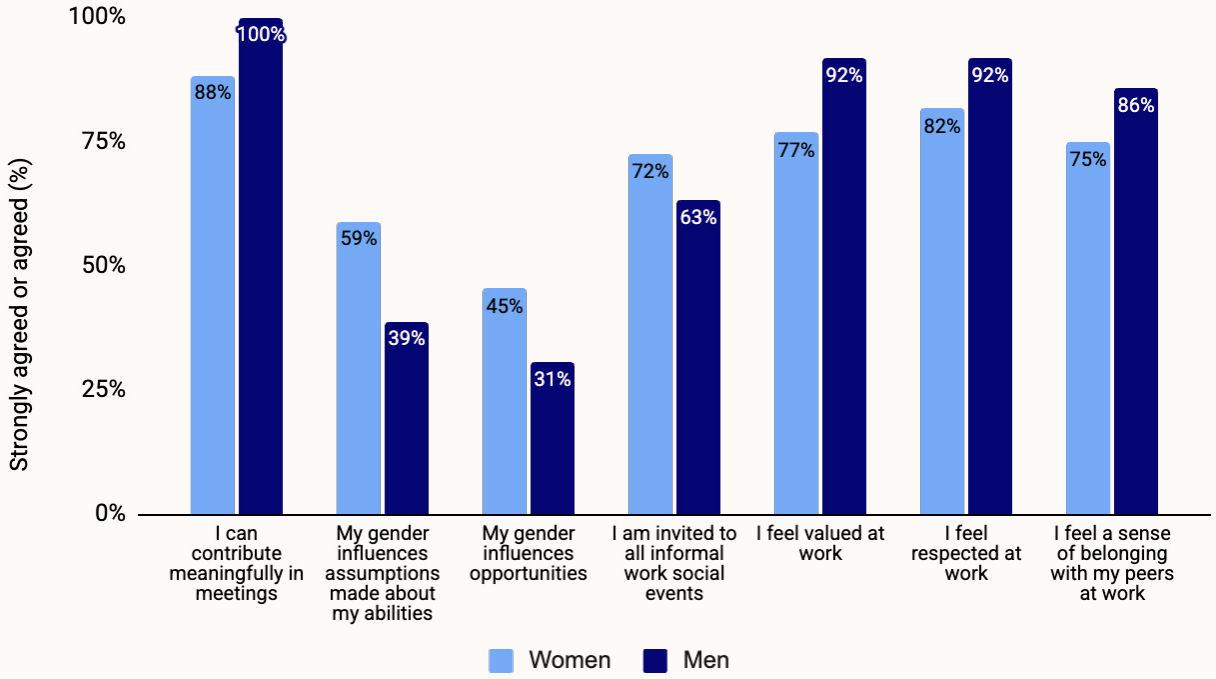
We include these findings and quotes to capture the experiences of those currently or previously working in cyber security. To represent the data accurately, we include the number of survey respondents to each question.

Inclusion and belonging

> "There are still some organisations that are very 'old school' in their way of thinking and nothing will ever change, however there are some progressive and encouraging organisations out there that are bucking the trend. Hopefully they become the norm."

The survey found that different genders experience the cyber security workplace differently. Women are less likely than men to feel a sense of belonging, they feel less respected at work, and are less able to contribute meaningfully in meetings (Figure 3).

Figure 3. Experiences of belonging, by gender



Source: Cyber 5050 survey. Respondents (n=212) were asked 'To what extent do you agree or disagree with the following?'.

Qualitative data reinforced these findings, with many women reporting feelings of isolation and exclusion. Respondents commonly revealed being ignored in conversations or being treated differently due to their gender. One individual noted that the culture also has consequences. She noted, 'it's a subtle feeling, nothing overt or easily identifiable, but there are moments where I sense a disconnect, as if I'm slightly out of place'.

Others shared the culture left them feeling withdrawn, either by working from home more frequently or speaking less in the workplace. One male respondent highlighted the impacts of a gendered culture on his sense of belonging, sharing that 'I have felt a lack of belonging when I have been included in very blokey conversations which are often very exclusionary towards women. Or worse, actively misogynistic. Those make me feel uncomfortable'.

> "At times I've felt a deep sense of alienation. I've observed that when I contribute ideas or insights, they're often received differently than if/when a male colleague says the same thing. I've also experienced being ignored or excluded in social conversations, even in areas where I'm genuinely knowledgeable and passionate. This creates a sense that I'm not welcome, or not perceived as credible."

Many women reported receiving biased assumptions around their interest in leadership opportunities. Some respondents expressed feeling undermined or overlooked for leadership positions due to their perceived skills and aptitude. One individual described feeling additional pressure and isolation being the only woman in the team and the burden of responsibility to push back on the assumptions made against all women.

Anecdotal findings reveal there is a stereotype that women perform feminised work while men undertake logical work. For example, some respondents felt they carried an unfair administrative burden due to the gendered expectation that women would carry out the 'glue work', with one sharing that 'women do most of the kitchen cleaning responsibilities'. Some women have reported experiencing double standards, where their similar behaviours were met with antagonism, while men exhibiting them were praised.

Hostile boys' club culture

> "I've been told to get back [in] my corner while the big boys talk."

Many felt belittled or humiliated by men, noting women were 'always outside of the boys' club'. Several described experiencing behaviours that reinforced traditional masculinity, such as centering informal social interactions around drinking and leisure, which alienated those who did not conform to these norms.

> "It is a zero-sum game. Creating privileges for any demographic [penalises] the rest. It creates the problem it's attempting to solve."

A minority of respondents expressed strong resistance to the topic, rejecting the existence of gender inequality in the industry. Some articulated concerns that initiatives aimed at gender equality disadvantage men, while one respondent rejected the validity of trans identities.

Intersectional exclusion

Many respondents reported experiencing more than one form of discrimination based on their identity or background, highlighting the need for holistic approaches to improve workforce diversity.

> "I complained to HR who gave me a letter about the racist slurs and bullying. The bully continues to stay while the bullied are asked to leave the org forcefully by HR and senior mgmt. This unfair law of not addressing the behaviours of racism and bullying by white men was made to save the perpetrators. How sick!"

Notably, respondents reported experiences of discrimination, exclusion and bias due to their race or cultural background. Several noted that the lack of gender and cultural representation exacerbated feelings of isolation and alienation among culturally diverse women. Some individuals had experienced casual racism and bullying, while others described being ignored and marginalised by Caucasian peers and leaders. Additionally, some individuals felt that their qualifications and skills were doubted because of their race, while others expressed frustration around being overlooked for opportunities in favour of less qualified candidates.

Many respondents also reported experiencing ageism in the workplace. Ageism was experienced by both older and younger respondents. A few older respondents highlighted that the industry is at risk of losing talented and experienced professionals as a result of age bias and a lack of support for women in their mid-life. Meanwhile, one young respondent described being excluded from social gatherings and being undermined due to receiving a constant focus on their appearance rather than work.

> "Please consider ageism. This industry is losing a lot of talent due to this painful issue that is not really acknowledged."

Several queer and gender diverse respondents highlighted the importance of being inclusive to all gender identities in gender equality initiatives. One transgender individual shared that their experiences after being perceived as a woman made navigating the workplace harder, expressing 'it would take much longer to establish credibility with clients, all those things made it much harder to maintain my position, despite the company being, on the face of it, quite supportive of women'. Another individual urged employers to '[en]sure that non-binary people are actually included in these initiatives, as we often feel like an afterthought or excluded from the initiatives that are supposed to be about improving gender diversity'.

Bullying and sexual harassment

Qualitative feedback suggested women in cyber security experience bullying and sexual harassment. The risk of bullying and sexual harassment commonly undermined women's feelings of safety, with many respondents expressing significant distress. One respondent stated that 'women have a list of safe men, and a list of unsafe men', demonstrating the severity of misconduct and undermining behaviours.

> "There is a high risk of predatory men seeking to gain coercive influence [over] women seeking to enter the industry."

Several respondents reported directly experiencing or witnessing bullying and sexual harassment. Respondents frequently reported being objectified by men, often receiving or knowing someone who had received inappropriate comments about their clothing, sexual jokes or casual sexism. One woman mentioned a male colleague making comments about her underwear during a social event, which led to her feeling unsafe and eventually relocating to avoid further harassment.

These findings suggest that some workplaces are still not meeting their basic legal responsibilities to keep employees safe. Laws such as the Respect at Work Act 2022 and Sex Discrimination Act 1984 (Cth) set clear standards to prevent harassment and discrimination. Under legislation, employers are required to take proactive steps, known as a 'positive duty' to prevent such incidents from occurring. The experiences highlighted in the survey indicate some workplaces are not following these standards, leaving employees unprotected and at risk.

Gender-based microaggressions

Microaggressions are 'seemingly innocuous verbal, behavioural or environmental slights against members of minority communities'.[30] Gender-based microaggressions are subtle, often unintentional actions or behaviours that communicate prejudice or bias against an individual based on their gender.[31] Microaggressions can vary in severity and can be considered as more serious offences such as bullying or sexual harassment. Crucially, if left unaddressed, microaggressions can enable a workplace culture that heightens the risk of serious incidents occurring.

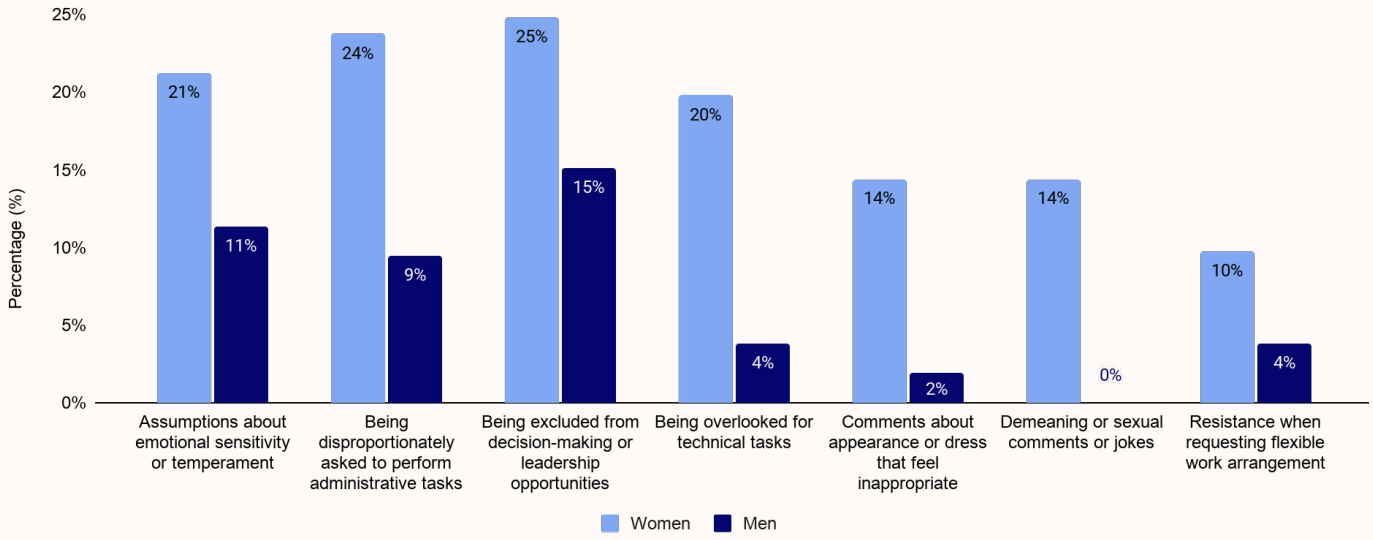
The survey found that women are more likely to experience a range of gender-based microaggressions at work (see Figure 4). Furthermore, men are significantly more likely to report never experiencing microaggressions.

Women are more likely than men to:

- face assumptions about their emotional sensitivity or temperament
- encounter inappropriate comments about appearance or dress, as well as demeaning or sexual comments or jokes
- be asked to perform administrative tasks
- be excluded from decision-making or leadership opportunities
- be overlooked for technical tasks
- face more stigma or resistance when requesting flexible work arrangements.

[30] Kalla (2023).
[31] Gartner (2022), p. 1.

Figure 4. Experiences of gender microaggressions, by gender

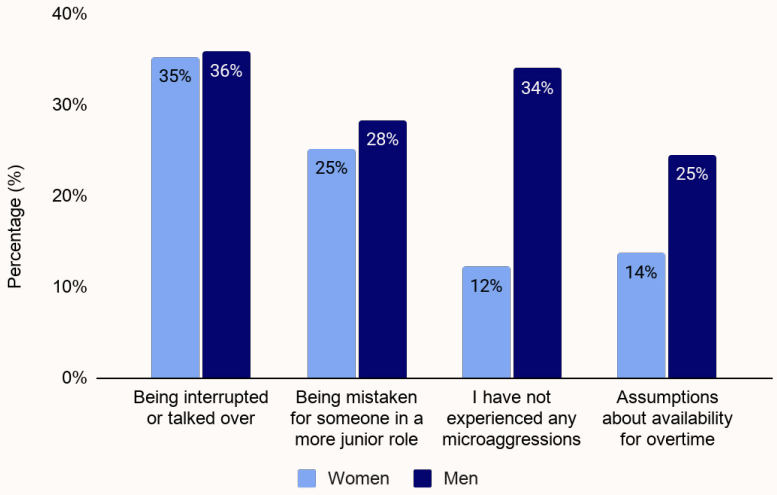


Source: Cyber 5050 survey. Respondents (n=212) were asked 'Have you experienced any of the following workplace microaggressions?' Of these respondents, n=163 identified as women and n=49 identified as men.

Men more commonly reported experiencing microaggressions around the assumptions about their availability for overtime (see Figure 5), in line with findings on the gendered nature of workloads explored later in this chapter.

Somewhat surprisingly, Figure 5 shows women and men reported similar rates of 'being interrupted or talked over at work', and of 'being mistaken for someone in a more junior role'. These are both microaggressions that are generally more commonly associated with women.

Figure 5. Experiences of gender microaggressions (cont.), by gender

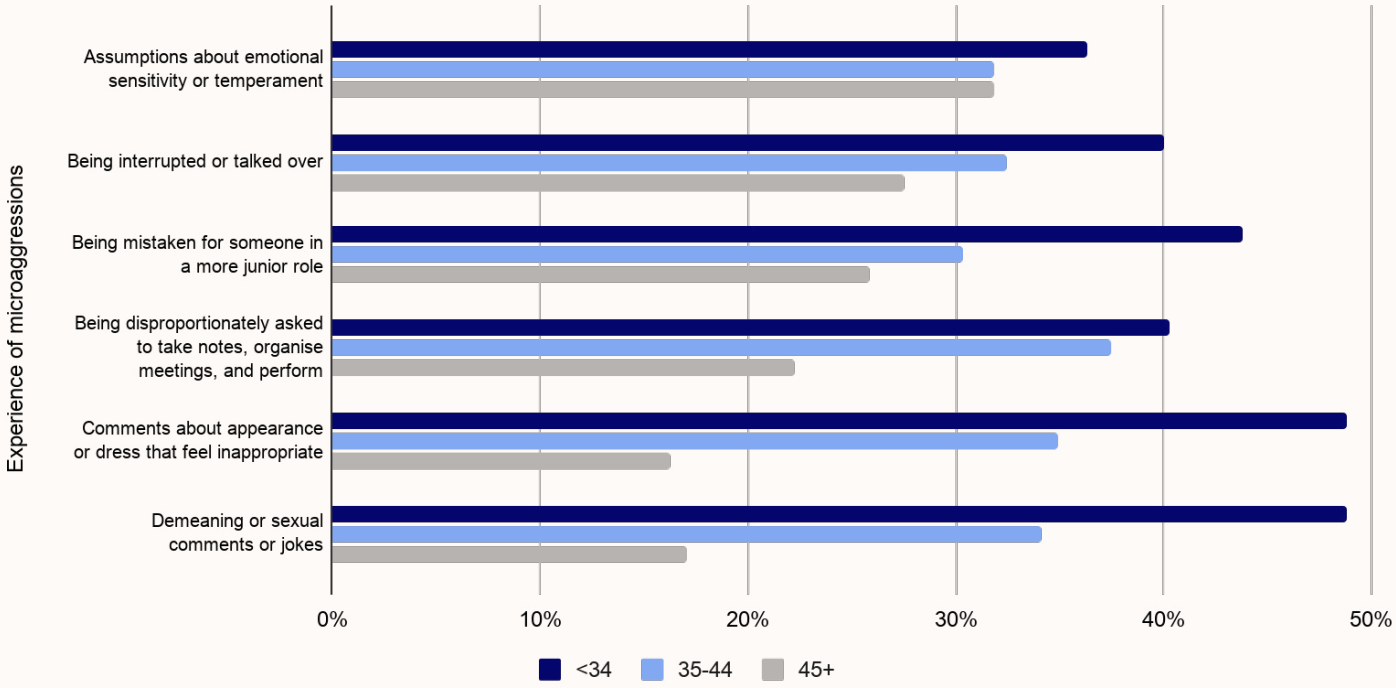


Source: Cyber 5050 survey. Respondents (n=212) were asked 'Have you experienced any of the following workplace microaggressions?' Of these respondents, n=163 identified as women and n=49 identified as men.

Respondents of different ages experienced microaggressions differently. Participants aged 34 or under more frequently reported experiencing microaggressions compared to those aged 35-44 or 45 and over. Figure 6 shows they were more likely to:

- face assumptions about their emotional sensitivity or temperament
- be interrupted or talked over
- be mistaken for someone in a more junior role
- be disproportionately asked to take notes, organise meetings, and perform administrative tasks
- receive comments about their appearance or dress that feel inappropriate
- receive demeaning or sexual comments or jokes.

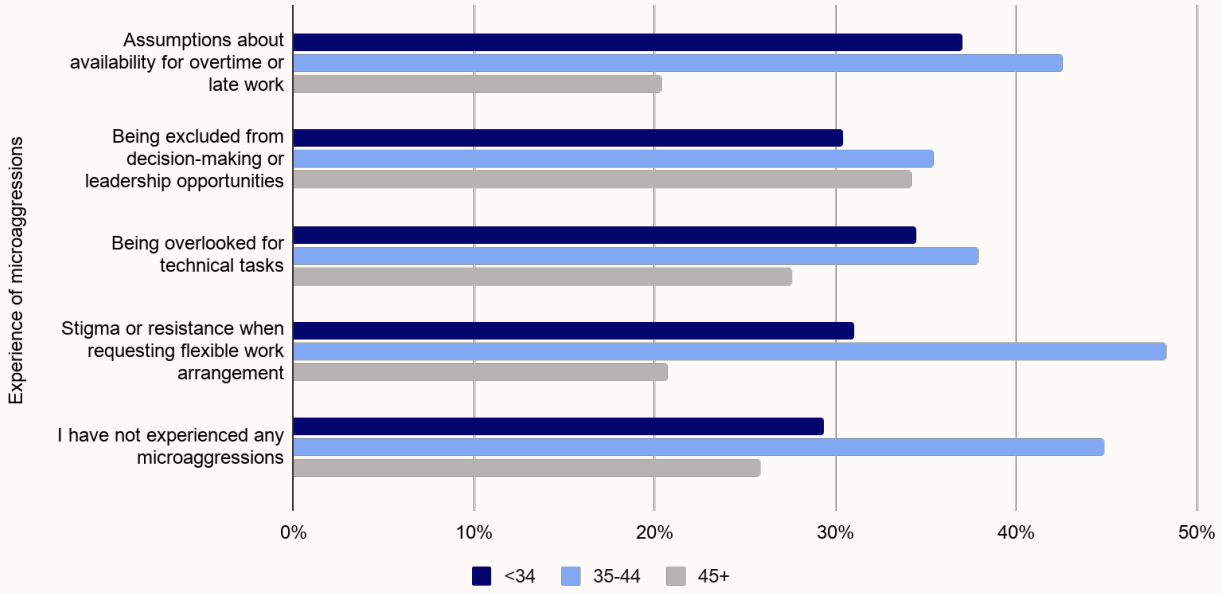
Figure 6. Experiences of gender microaggressions, by age



Source: Cyber 5050 survey. Respondents (n=223) were asked 'Have you experienced any of the following workplace microaggressions?'.

Respondents aged 35-44 reported facing more assumptions about their availability for overtime and more stigma when requesting flexible work arrangements than respondents aged 34 and under or 45 and over.. They were also more likely to be overlooked for technical tasks, despite potentially having considerable work experience (see Figure 7).

Figure 7. Experiences of gender microaggressions (cont.), by age

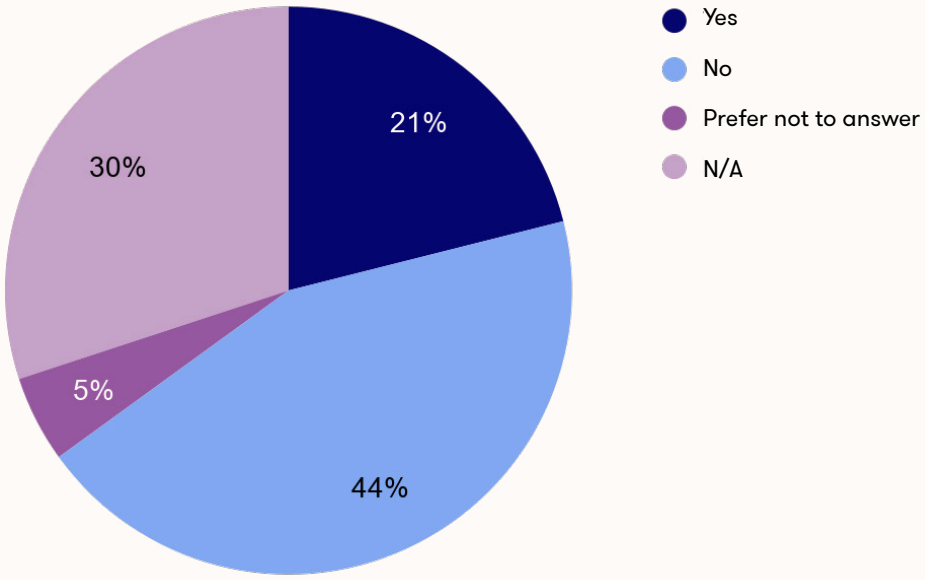


Source: Cyber 5050 survey. Respondents (n=223) were asked 'Have you experienced any of the following workplace microaggressions?'.

Reporting microaggressions

Microaggressions are subtle, everyday forms of discrimination, and people do not always choose to report them. That said, as these experiences have varying degrees of impact and severity, 21 per cent of respondents reported incidents (see Figure 8).

Figure 8. Proportion of respondents who reported experiences of microaggressions



Source: Cyber 5050 survey. Respondents (n=212) were asked 'Did you report any of these incidents?'.

Qualitative feedback reveals that many women who speak up about experiencing microaggressions are further alienated, reprimanded or given advice that places the responsibility back on women. Additionally, some respondents highlighted a lack of accountability for perpetrators and the lack of support for victims reflects a culture where people managers are passive bystanders, enabling such behaviours to be tolerated.

> "As the victim or receiver of these [microaggressions] I was subject to more training on DEI instead of the perpetrator. It made me think twice about reporting future incidents."

Impacts of microaggressions

Qualitative data highlights that gender-based microaggressions have far-reaching implications for the cyber workforce. Respondents shared that these experiences have led to an erosion of confidence and lower productivity. For example, some respondents expressed feeling exhausted, unimportant and doubting their own skills.

> "One person's behaviour and attitude towards me regularly makes me feel unimportant. I am confident in my abilities, but they consistently make me doubt them. Every time I am in a meeting with this person, I find myself anxious to speak, so [I] have stopped contributing to those meetings."

Many respondents reported leaving workplaces due to the cumulative effects of microaggressions. Some expressed feeling demoralised or experiencing mental health challenges as a result. These findings highlight the often severe and insidious impacts of gendered microaggressions.

> "I felt completely excluded and unvalued and thought I should give up working in Cyber Security. I didn't want to attend the workplace and always feared his meetings where people might speak up as they tended to turn ugly and this became quite depressing the longer it went on for."

Others felt like these negative experiences built their resilience and perseverance by making them work harder. A few respondents said it 'Made me more determined to prove myself' or made them stronger so they could eventually upskill into a leadership position. However, some felt women needed to work twice as hard to prove their worth. Others reported growing desensitised to microaggressions, with one sharing 'that's how it is and you accept it or find another job', and another reporting they 'spent over 25 years just dealing with it'.

Workload and burnout

> "I just flop in an emotionally unstable way between trying my hardest to prove I belong in this industry when it is burning me out, and not caring and becoming disengaged, quickly followed by large amounts of guilt for taking that approach."

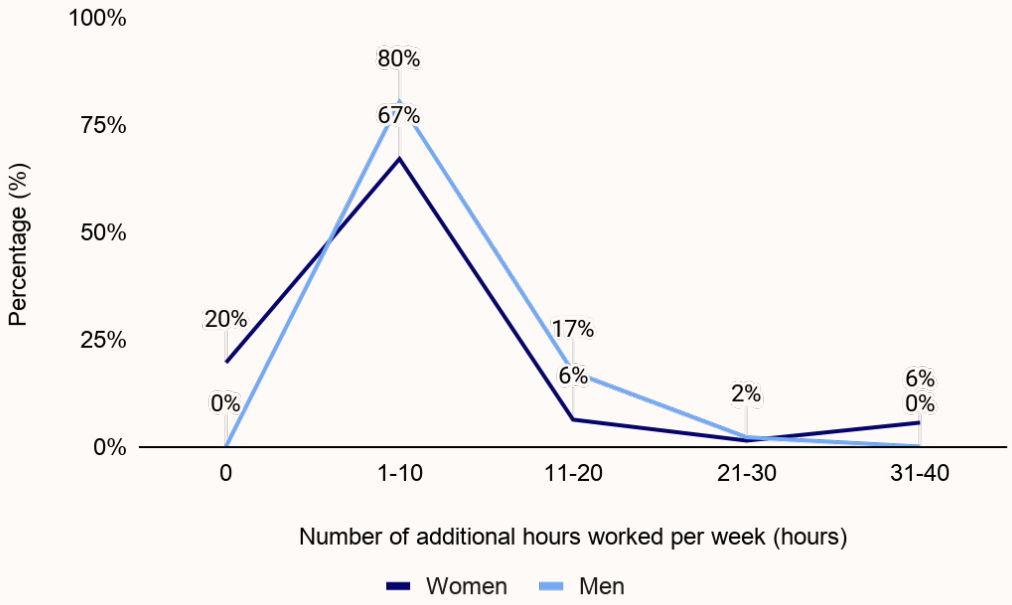
Beyond Blue explains burnout as when a person feels emotionally, physically and mentally exhausted from excessive demands at work and/or in their personal life, and notes symptoms include feeling physically and emotionally exhausted, negative about work, and less effective at work.[32]

Cyber5050 survey data found that 85 per cent of cyber professionals reported working additional hours per week. Figure 9 compares the number of additional hours worked per week by gender, revealing distinct patterns between women and men. Men report working more extra hours than women, with 80 per cent working an extra 1 to 10 hours per week compared to only 67 per cent of women. No men report doing no additional hours at all, compared to 20 per cent of women.

However, only women (6% of respondents) report working an additional 31 to 40 hours per week. It is not clear from this research what drove this finding, and we recommend further research to interrogate the drivers of extreme hours in cyber security.

[32] Beyond Blue (2025).

Figure 9. Number of additional hours worked per week, by gender



Source: Cyber 5050 survey. Respondents (n=200) were asked 'On average, how many additional hours do you work per week, beyond your FTE status?'.

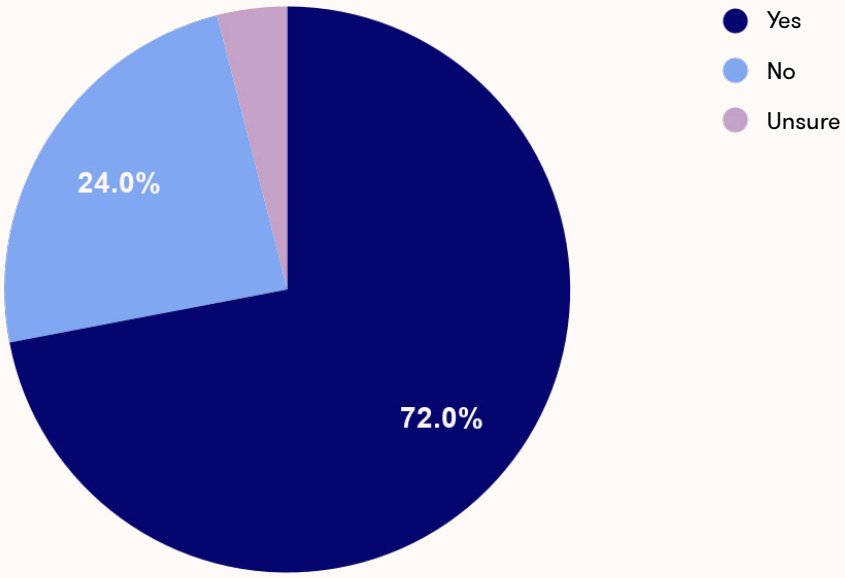
Qualitative findings show that despite women working less hours than men, some still struggle with the intensity of the workload, feeling the need 'to prove myself more than my peers'.

> "It's exhausting [that] I am working twice as hard and being told I'm half arsing it."

Almost three-quarters (72%) of respondents reported experiencing burnout at some point in their career in cyber security, and 4 per cent were unsure (see Figure 10).

Responses are similar across genders, with 73 per cent of women and 72 per cent of men reporting burnout. Qualitative feedback highlights that parents and caregivers are particularly impacted by long working hours. Many reported wanting more awareness and support for work-life balance, such as stronger parental leave policies and limiting after-hours activities.

Figure 10. Experiences of burnout while working in cyber security

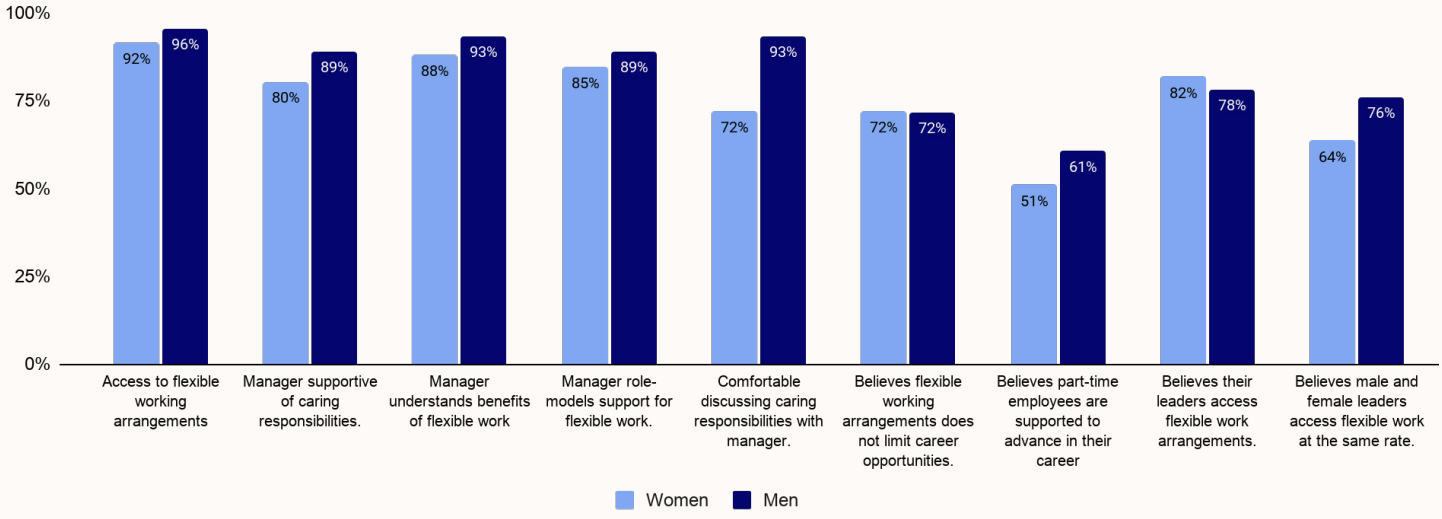


Source: Cyber 5050 survey. Respondents (n=200) were asked 'While working in cyber security, have you experienced burnout?'

Access to flexible working

Figure 11 compares access and experiences to workplace flexibility by gender, showing relatively similar patterns between women and men. This is promising, and reflects the potential for the industry to reduce barriers and provide flexible working arrangements.

Figure 11. Experiences of workplace flexibility, by gender



Source: Cyber 5050 survey. Respondents (n=200) were asked 'To what extent do you agree or disagree with the following statements?'.

Surprisingly, 93 per cent of men report feeling comfortable discussing their caring responsibilities with their manager, compared to 72 per cent of women. Further research is required to understand this finding, which is at odds with broader research from Australian workplaces that finds men face more stigma than women when requesting flexible working arrangements.[33]

Despite overall good access, all genders report concerns about the impact that utilising these entitlements may have on their career progression:

- 25 per cent of men and women believe flexible working arrangements may limit their career opportunities.*
- Only 51 per cent of women felt that part-time employees are supported to advance their careers, a notable barrier for women who are more likely to work (or want to work) part-time.
- 27 per cent of women respondents felt that male and female leaders do not access flexible arrangements at the same rate.*

Additionally, qualitative feedback highlights that access to flexible working is not possible for everyone. Some flexible arrangements may not be possible for carers juggling multiple responsibilities or individuals in '24/7 on-call' operational positions due to the inherent demands of their roles.

*This finding excludes those who responded 'not applicable'.

[33] Sanders et al. (2015).

Key findings

Stereotypes, inclusion and belonging

- The boys' club culture within parts of the cyber security environment has profound consequences for many women, as well as some men.
- Individuals within cyber security also face discrimination based on age, race, and gender identity.

Gender-based microaggressions

- Women and younger individuals are more likely to experience microaggressions compared to men and those who are older.
- Women face assumptions about temperament, inappropriate comments, and exclusion from technical or leadership tasks. Men more often face assumptions about overtime availability. Younger respondents experience more frequent microaggressions.
- One in five respondents (21%) report microaggressions, which suggests the unreported rate is much higher. Reporting microaggressions often results in negative consequences for the person who made the report and/or inaction from management.
- As a consequence of microaggressions, survey respondents report reduced confidence, mental health strain, burnout, and attrition.

Workloads, burnout and flexible work

- A majority of cyber professionals work additional hours per week (85%) and report high rates of burnout (72%).
- These high workload demands have negative impacts on individuals, and in particular women who often have a higher share of caring responsibilities.
- While both genders have access to flexible work options, women feel less comfortable discussing them with their managers.
- There remain specific barriers to flexible work for people in key cyber roles.

2. HELPING WOMEN ENTER CYBER SECURITY

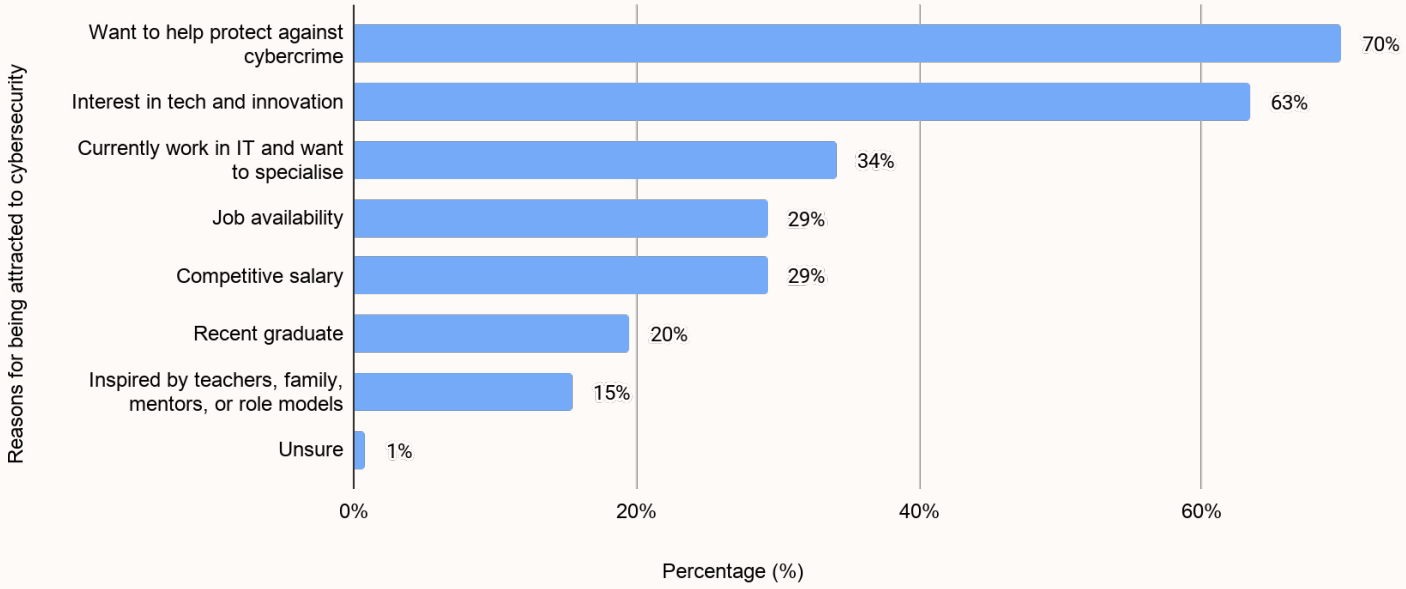
This chapter outlines the cultural and structural barriers to attracting and recruiting a gender diverse cyber security workforce. It also showcases specific suggestions for improvement that survey respondents provided.

Data from this chapter includes feedback from respondents who are working in, previously worked in or want to work in cyber security in Australia.

Perceptions and stereotypes

The most common reasons respondents were attracted to the industry were a desire to help protect people and organisations from cyber crime (70%) and an interest in technology and innovation (63%). Moving into cyber security from a current IT role is also a significant motivation. These findings were comparable for women and men.

Figure 12. Motivations to join cyber security



Source: Cyber 5050 survey. Respondents who aspire to work in cybersecurity (n=123) were asked 'Which of the following attracts you to work in cyber security?'.

However, it is clear that cyber security has a reputation as a male-dominated industry, with 89 per cent of respondents agreeing that 'most people working in cyber security are men'.

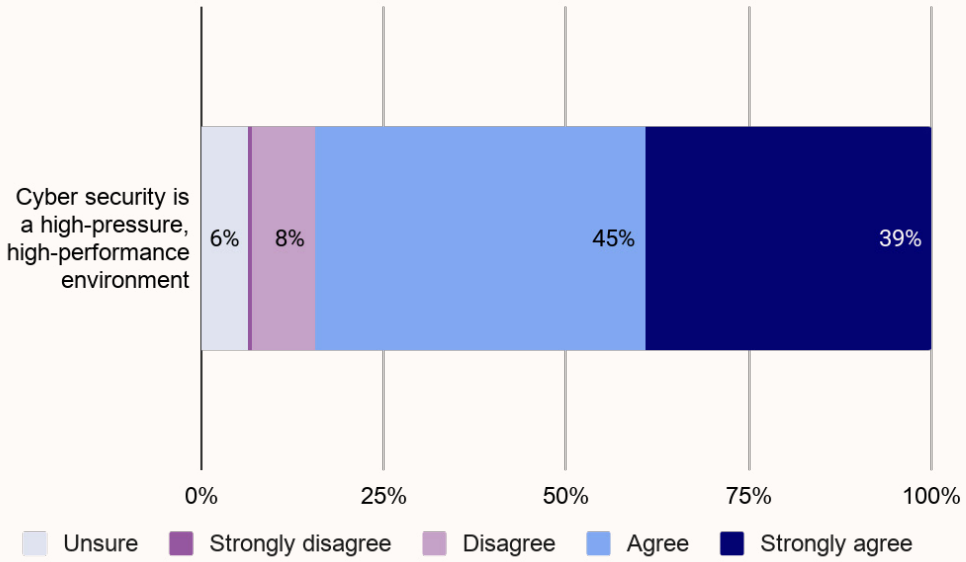
> "There is a deep assumption by men in this industry that women are just quota hires."

Stereotypes about 'who belongs' in the industry play an important role. For example, a couple of respondents warned that the image of a hooded man in front of a computer in a dark room, which is often associated with the cyber security profession, can hinder women and girls from being attracted to the industry.

> "Continual work to change the image of the industry, unfortunately IT/Cyber has very much still the same image of the male IT nerd, i.e. IT Crowd If you type cyber security into youtube, many thumbnails which include people are often men. We just need more women and gender diverse examples which are known and expected when it comes to this industry."

Additionally, 84 per cent of respondents agreed that cyber security is a 'high-pressure, high-performance environment' (see Figure 13). Qualitative findings indicate this can create an intimidating image of the industry.

Figure 13. Perceptions of cyber security as a high-pressure environment



Source: Cyber 5050 survey. Respondents (n=283) were asked 'To what extent do you agree or disagree with the following?'.

Some reported feeling uncomfortable applying to jobs in cyber security due to 'isolating' experiences of being the only woman in interviews or university classes. Others reported experiencing imposter syndrome and doubting their skills against male applicants.

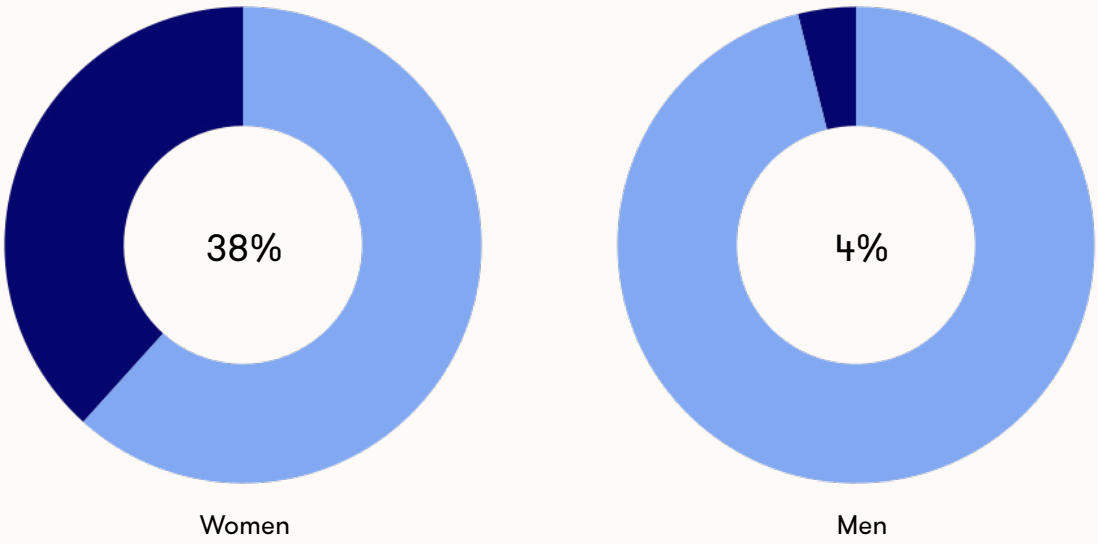
> "It is incredibly intimidating to apply for work in an organisation where there are no/few non-male employees, particularly where the only non-male interviewees are there [from] a HR position as opposed to a technical position."

Perceptions of cyber security as an exclusive profession are exacerbated by the low visibility of women leaders. This can further prevent women and gender diverse people from entering. Without visible role models and successful examples of women thriving in leadership roles, there is a risk that harmful perceptions towards women could manifest in their absence. For example, several respondents reported an underlying view among staff that women are 'token' or 'quota hires'.

Bias in recruitment

Gender bias in recruitment can manifest in many ways, all of which dissuade capable applicants from applying. Figure 14 illustrates that even women who are motivated to join cyber security face more barriers during recruitment compared to men.

Figure 14. Proportion of respondents who experienced barriers to enter cyber security, by gender



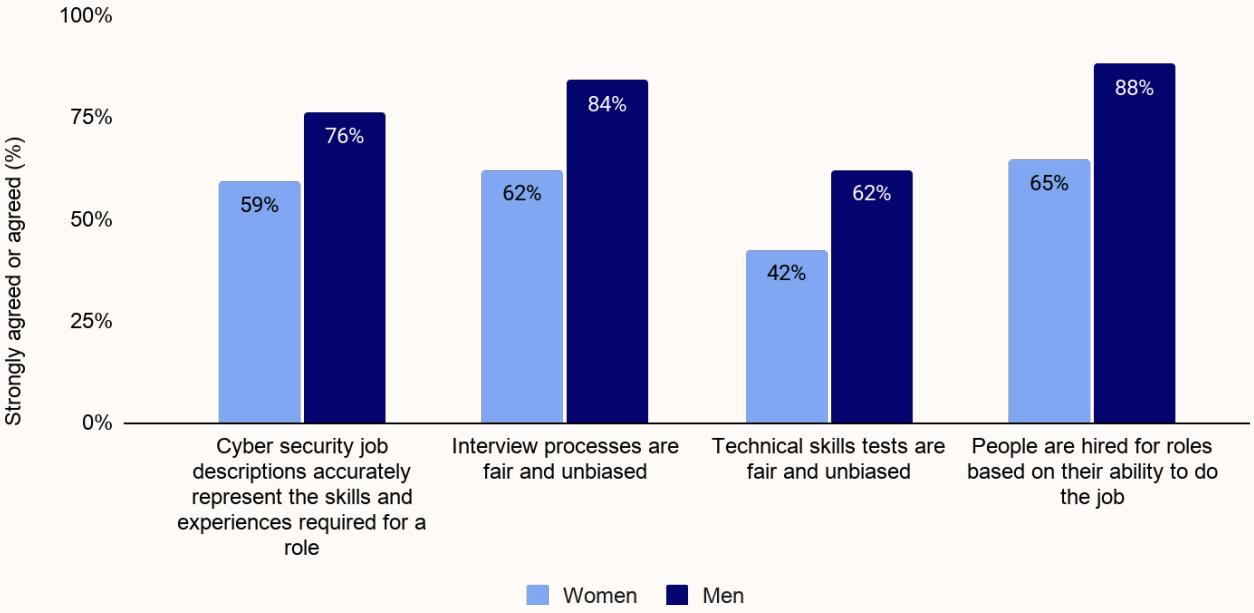
Source: Cyber 5050 survey. Respondents (n=285) were asked 'Do you feel like you experienced any real or perceived gendered barriers when entering cyber security?'.

These barriers were felt more intensely by individuals with prior cyber security experience seeking re-entry into the workforce (60%) compared to those presently working in (31%) or aspiring to join the field (29%). Career breaks for childcare or other caregiving duties were frequently cited by respondents as major obstacles to re-entering the workforce, which may partly explain this trend. These are further interrogated in the Work Experience and Career Break Stigma section.

Additionally, respondents aged 45 and over were more likely to experience gendered barriers during entry (39%), compared to those aged 35-44 (31%) or 34 and under (24%), indicating ageism could factor into recruitment bias.

Critically, perceptions of bias differ between women and men, with women less likely to agree that recruitment processes are fair compared to men across all measures. Only 62 per cent of women agree that 'interview processes are fair and unbiased', compared to 84 per cent of men (see Figure 15). Similarly, women are less likely to agree that 'people are hired for roles based on their ability to do the job' compared to men.

Figure 15. Perceptions of the recruitment process, by gender



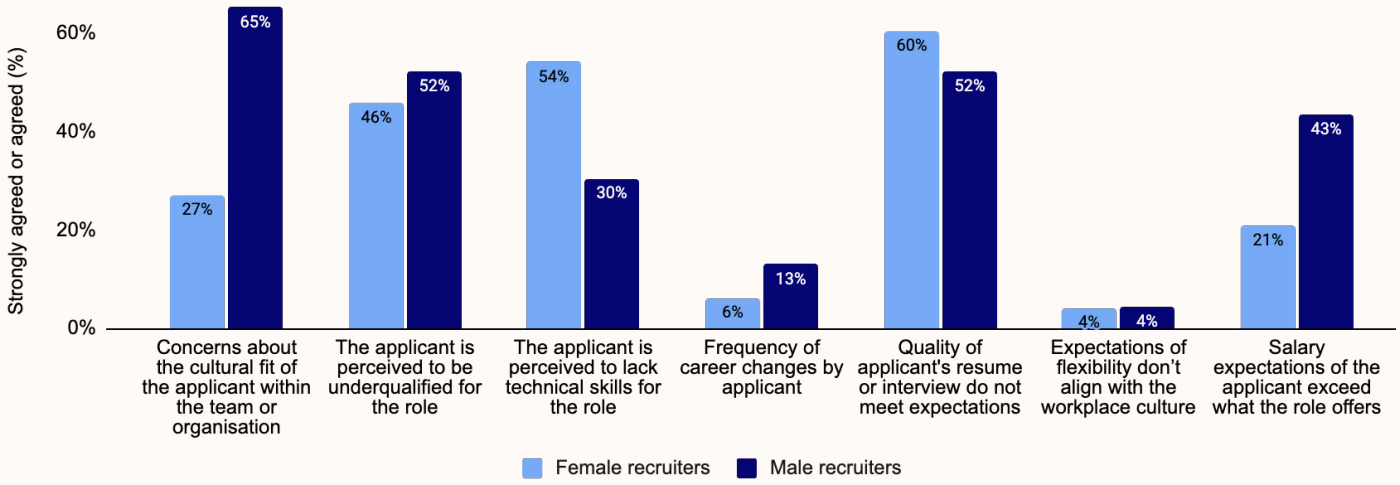
Source: Cyber 5050 survey. Respondents (n=214) were asked 'To what extent do you agree or disagree with the following?'.

Differences between male and female recruiters

Figure 16 suggests that recruiter gender may shape how candidate strengths and weaknesses are evaluated, potentially influencing hiring outcomes in subtle ways.

For example, male recruiters are more likely to place more emphasis on cultural fit, with 65 per cent noting this as a reason for rejection, compared with just 27 per cent of female recruiters. Differences also appear in perceptions of technical competence (see further analysis below).

Figure 16. Most common reasons why recruiters do not select entry-level applicants



Source: Cyber 5050 survey. Male and female respondents with hiring responsibilities (n=71) were asked 'What are the most common reasons entry-level applicants are not selected?' Of the hiring managers n=48 identified as women or female and n=23 identified as men or male.

The role of affinity bias

Qualitative data suggest that unconscious bias is pervasive in recruitment. Several respondents highlighted that affinity bias is common, with hiring managers favouring applicants with similar backgrounds, behaviours and attitudes. One respondent described this as 'cronyism'.

A few respondents stressed the importance of merit-based recruitment processes that use fair assessment criteria rather than making decisions based on a person's identity.

One consultation participant challenged this view, noting that meritocratic processes can be flawed and can 'ignore the layered impacts when people begin their cyber journey, such as financial and time pressures that are external to a person's capabilities'.

> "Treat everyone the same regardless of gender. Hire and promote based on attributes that are important to the role, which gender is not."

Excessive focus on technical abilities

Respondents and consultation participants frequently raised a common stereotype in the industry that men have valuable 'technical skills' while women have less valuable 'soft skills'.

For example, one respondent revealed there are 'very real, substantiated concerns that there are people in hiring positions [who] hold the view that men are innately better suited to technical roles due to 'biological differences' being more logical or rational'.

Several consultation participants noted that this belief underpins why women often 'self-select out' of cyber security roles, despite having valuable transferable skills. One participant said that transferable skills, such as communication and analytical skills are less valued because they are associated with women's skills.

Respondents emphasised 'the human aspect is so important', noting that 'cyber needs better communicators, people who can think outside of the box, people who can adapt and lead others'. However, it is clear that current recruitment processes over-emphasise technical skill, as one respondent felt that jargon was 'weaponised' during recruitment.

One consultation participant shared similar experiences, noting that 'being technical is being prized above often to the detriment of the industry'. Others shared experiences of being disregarded despite having technical experience, often being perceived as 'not technical enough'. Another respondent observed applicants being 'filter[ed] out for not knowing specific tool[s]' that could be learnt on the job as a result of prioritising 'buzzwords' and the ability to use technical tools over diverse work experiences.

> "I've missed out on jobs I've been absolutely qualified for because the hiring managers would prefer to hire a man who they are more comfortable with. Too technical, not technical enough… I've gotten all the excuses, when they want to give the role to their male friends."

A few others noted that hiring managers who do not have a technical cyber security background may overestimate the technical skills required for a role, which may risk disadvantaging some candidates.

Work experience and career break stigma

Respondents explained that the focus on prior industry experience in recruitment acts as a considerable barrier to entry for women.

> "So I've done a bachelor's of IT (Comp Sci) and finished my Cert IV in Cyber. Looking at job ads can be discouraging as they require many years of experience in industry or emphasise the need for certification. [There] doesn't seem to be entry level… job titles."

Several respondents who had studied cyber security highlighted that entry-level positions often required years of experience, locking out early-career graduates and those with minimal experience before taking a career break due to pregnancy and parenthood. Others emphasised the lack of consideration for those who have completed training and certifications in favour of those who already work in the field.

Some respondents felt 'punished' for taking a career break to care for their family or children. A few highlighted the stigma and bias that surfaced when recruiting women in their 'childbearing' years due to the assumption that they may take parental leave.

> "It was a conscious decision to step away from full-time work when family needed focus, and now to focus on full-time work again. Women self-exclude. We step away when other things need focus, and then step back again when we can give our careers 100 per cent focus. Please DON'T punish us for needing to step away for a time. Give us a chance."

Some reflected that having a career gap on their CV significantly reduced their ability to secure interviews, while others noted recruiters prioritise individuals who have 'done their time and learned their craft' over those who have taken career breaks. As women continue to predominantly shoulder primary caring responsibilities in Australia,[34] career break bias has a clear gendered impact.

> "I'm not going to apply for anything in cyber security until I feel more confident in my current role (software developer) and skill set."

As a result of these barriers, some women reported feeling a lack of confidence when applying for cyber security roles. Some had an intention to apply for roles once they felt more confident, while others noted feeling less confident after applying for roles, fearing further disappointment and rejection.

Difficulty accessing flexible options

> "Being open and transparent throughout the recruitment process about flexible working practices and initiatives underway to help support women in the industry."

Access to flexible working arrangements is no longer a nice-to-have, but a must-have in order to grow a gender-equitable workforce.

Respondents shared that women often struggle to find roles that allow for flexibility without compromising their professional aspirations. For example, some reported that a lack of available part-time opportunities prevented mothers and carers from returning to work after a career break. One consultation participant revealed that she 'had to quit [her] 10-year job at a well-known IT provider after having [her] baby, because they said [she] could not come back to [her] role part-time'.

[34] Workplace Gender Equality Agency (2025).

At the same time, a few participants shared positive examples of how organisations supported them to enter or continue working in cyber security, highlighting that this is not only possible but directly linked to positive outcomes for women. One reflected that her organisation helped her find a role that allowed her to work flexible hours after she moved overseas, while another shared that her organisation found her a part-time role after returning from maternity leave, so she could stay.

Others expressed a desire for opportunities to job share roles that cannot be made part-time, noting this is not possible in all roles.

> "I also think we need to come up with out of the box thinking to allow more women into the workforce like job share, more options for night time child care also subsidised by the government for shift workers."

One respondent highlighted that flexible working practices such as the ability to work from home, parental leave and other flexible working policies should be transparently communicated throughout the recruitment process to encourage more women into the industry.

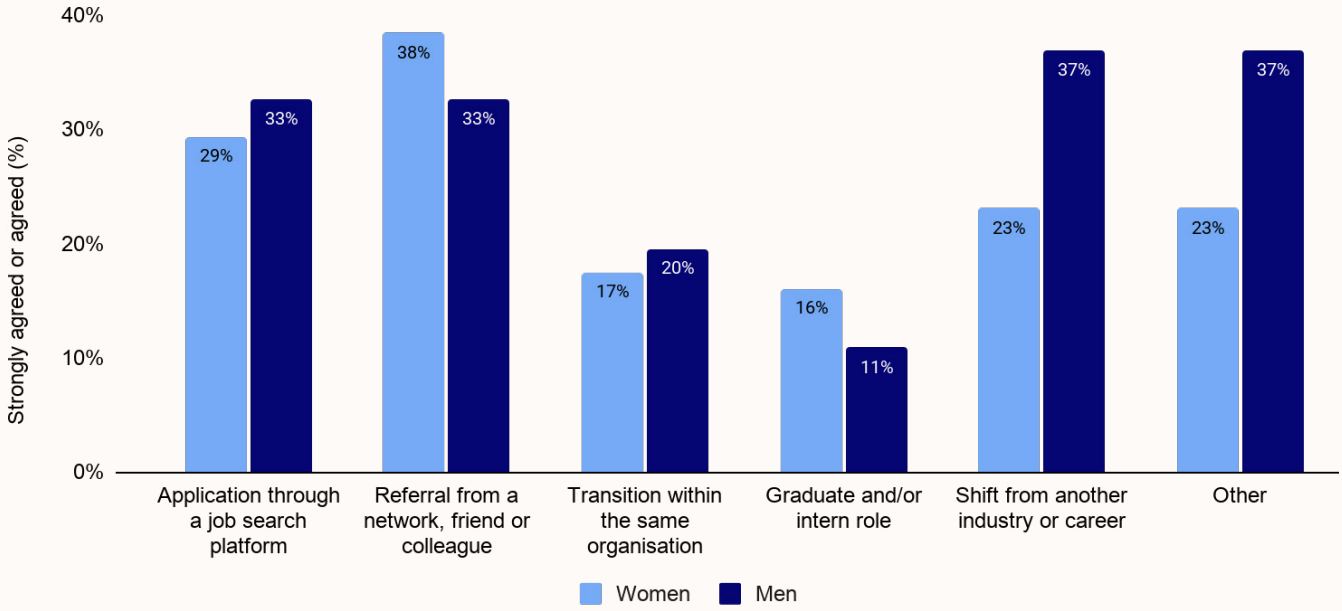
While flexible working and part-time arrangements are critical for enabling women's workforce participation, they can become a 'double-edged sword' if men are not equally taking up flexible work arrangements. Respondents highlighted that men's uptake of flexible arrangements is important to encourage their participation in household and caregiving responsibilities to support women's employment.

Limited pathways to entry

Figure 17 demonstrates that pathways entering cyber security varied by gender.

Based on data on those who currently work in cyber security, women were more likely than men to secure employment via a referral from a network or colleague (38% compared to 33%) and a graduate or internship program (16% compared to 11%). Men were more likely to secure employment via all other pathways.

Figure 17. Pathways taken to secure employment in cyber security, by gender



Source: Cyber 5050 survey. Respondents who currently work in cybersecurity (n=200) were asked 'Which of the following employment pathways did you take to secure your current role?'.

Many respondents aspiring to enter the field shared experiences of struggling to find entry-level opportunities after completing university or vocational training. Participants expressed feeling discouraged after applying for roles that demanded experience beyond what was expected for an entry-level position, reporting it's 'unclear where you would really start after study'.

> "I wish there were more opportunities for career changers. I am committed to transition to cyber security and I believe I bring valuable transferable skills to the field. In saying that, I find it's impossible to get an interview."

Figure 17 shows that men are significantly more likely than women (37% compared to 23%) to secure employment in cyber security after shifting from another industry. One consultation participant said, 'people don't know how to get in - they don't think it's advertised enough in different industries'.

Suggestions from respondents

Throughout this research, respondents offered a wide range of suggestions to address the barriers to entering cyber security and build a more gender-equal workforce. These suggestions are summarised below, and broadly align with existing Australian research on leading practice for inclusive recruitment.

Embed inclusive recruitment practices

Respondents suggested the following strategies.

- Use inclusive language in job advertisements, including gender-neutral language that does not dissuade women from applying; greater recognition of transferable and non-technical skills; greater promotion of flexible working and leave policies.
- Review role descriptions and criteria, ensuring these accurately reflect the requirements of the role (rather than, for example, the duties and CV of the role's predecessor); that non-technical skillsets are included; and that overseas qualifications are recognised wherever possible.
- Use inclusive hiring practices, such as blind resume reviews and gender neutral or women-only interview panels.
- Ensure hiring managers have done unconscious bias training and understand intersectional barriers to employment to actively ensure the safety and inclusion of culturally diverse women, older women and gender diverse applicants.
- Build confidence, by providing feedback on all applications to ensure applicants are not discouraged from applying for future opportunities and by actively encouraging women employees to apply for roles.

Build supported recruitment pathways

Many respondents advocated for more funding to expand pathways for women into cyber security. Work-integrated learning programs such as industry placements, internships and traineeships were commonly cited as 'legitimate and solid' pathways to gain 'on-the-job' experience. Respondents saw this as highly valuable given the strong focus on industry experience and the otherwise limited opportunities available for entry-level candidates to build their experience.

Other suggestions included establishing more internships for women of colour, women with working visas, and international students, as well as promoting initiatives that showcase talent, such as 'hackathon'-style challenges.

Key findings

Bias in recruitment

- The perception of cyber security as a male-dominated profession continues to limit women and girls engaging with cyber security.
- Gender bias in recruitment creates a serious barrier for women and gender diverse people entering the industry. This bias manifests in a number of ways, including as unconscious affinity bias and an over-emphasis on technical skills and work experience, as well as career break stigma.
- The stereotype that women are less technical and possess less desirable skills than men remains a significant barrier. Not only does this prevent opportunities for career development, it also leaves many women feeling unmotivated and undervalued.

Recruitment pathways

- Despite the demand for skilled workers, there are limited pathways to enter cyber security. Women were more likely to enter through a referral from a network or a graduate program, while men were more likely to enter by transitioning from the same organisation or industry, a job search platform or industry programs, self-employment or targeted recruitment.
- Promoting flexible working arrangements and offering a range of employment types from the outset can enable more women to join or return to the workforce. Part-time opportunities, job-sharing and remote working were the most commonly sought arrangements.
- Respondents offered a range of suggestions to embed inclusive recruitment practices and to build supported pathways to enter the profession. Suggestions included:
    - reviewing and improving job descriptions to embed inclusive language
    - requiring unconscious bias training for managers
    - providing feedback to applicants
    - expanding pathways to entry through work-integrated programs, scholarships and mentoring initiatives.

3. HELPING WOMEN STAY IN CYBER SECURITY

Once women enter the cyber security industry, barriers to staying and progressing into leadership persist. This chapter discusses the obstacles to retention and strategies to build an inclusive workplace culture.

Data from this chapter includes feedback from respondents who are working in, previously worked in or want to work in cyber security in Australia.

Perceptions of career opportunities

Overall, the data highlights persistent gender differences in how progression opportunities are perceived, with men consistently expressing more positive experiences and stronger institutional support than women (see Figure 18).

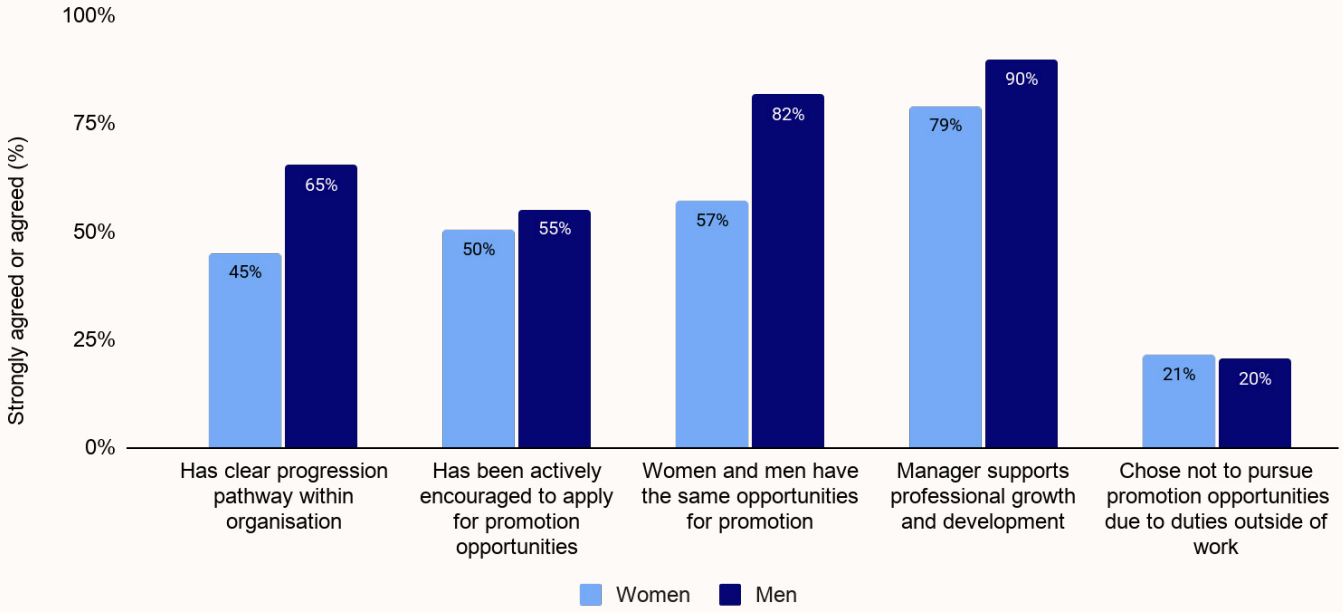
Women report less positive experiences than men across most metrics, highlighting a perception gap between genders. Notably:

- 45 per cent of women feel there is a clear progression pathway within their organisation (compared to 65% of men)
- 57 per cent of women believe women and men have the same opportunities for promotion (compared to 82% of men)

Similar proportions of women and men report receiving active encouragement from their managers to apply for promotions. Managerial backing for professional growth and development is more widely felt across both genders, with 79 per cent of women and 90 per cent of men agreeing, although again, men report more positively.

Interestingly, when it comes to personal barriers, such as not pursuing promotion opportunities due to duties outside of work, the responses are nearly identical, showing that external responsibilities affect both groups similarly.

Figure 18. Experiences of progression opportunities, by gender

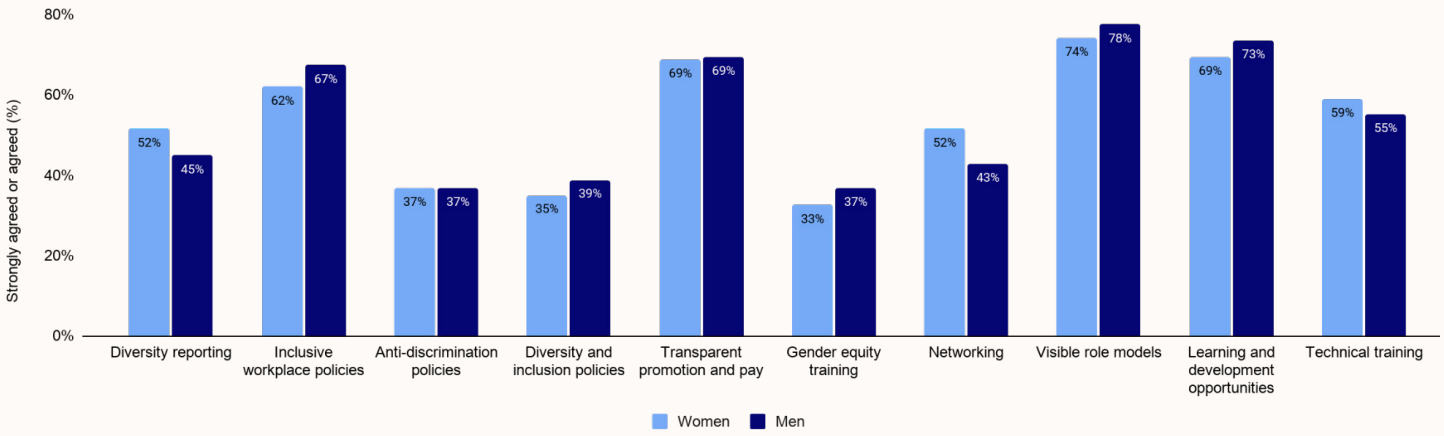


Source: Cyber 5050 survey. Respondents (n=212) were asked 'To what extent do you agree or disagree with the following statements?'.

Positive leadership and role models

Figure 19 illustrates the types of support perceived as the most useful to retain women by gender, reflecting similar patterns between women and men. Data highlights the important role that positive leaders and opportunities for development play in retention and progression of gender diverse workforces.

Figure 19. Retention supports, by gender



Source: Cyber 5050 survey. Respondents who previously and currently work in cybersecurity (n=212) were asked 'Which of the following do you think would support retention for women and gender diverse people in cyber security?'.

> "In credit to my Senior leadership who cut through a lot of the barriers to create an environment [where] I was genuinely empowered to be firm and robust against the challenges as they presented."

Both women and men identified the most valuable support to retain women is having visible role models in cyber security, affirming how critical it is to see others like them thriving in senior or technical positions. This is reinforced by qualitative feedback, which highlights the significant impact of positive leadership examples on respondents' sense of belonging and inclusion, which has an important effect on retention.

Mentoring and learning opportunities

Both genders highlighted learning and development opportunities, suggesting that respondents see significant value in creating clear pathways to upskilling and professional advancement. This is further emphasised by qualitative insights that highlight subsidised training opportunities, clear progression pathways and opportunities that promote women's confidence can encourage retention and growth.

At the same time, a few respondents highlighted the significantly higher workload expectations for leaders could hinder some from taking up these opportunities. Enabling job sharing and complementing high workloads with flexible arrangements is thus crucial to minimise the impact and enable women to navigate more demanding positions.

Several respondents noted that formal mentoring programs and informal peer mentoring make 'a difference for employee[s] to be recognised and be guided daily to show that managers value and care for their future progression, even at 1 per cent effort'. This is also established in existing research that demonstrates mentoring can have a profound impact on sustaining women in cyber security through role modelling and having a supportive network.[35] A few respondents also suggested implementing buddy systems 'so that people don't feel isolated or alone' and ensure new employees are 'comfortable approaching someone to ask 'silly' questions'.

[35] RMIT University (2023), p. 41.

Personal learning and short courses were commonly reported as the most impactful ways respondents prepared for the job. Many found self-paced learning such as microskilling programs and short online tutorials and workshops beneficial, particularly in helping them expand their knowledge across different cyber fields. However, one respondent pointed out that there are also 'a lot of useless, predatory micro courses' in the industry, indicating that not all courses are valuable. Nonetheless, respondents emphasised that access to continuous training opportunities can help employees maintain and adapt their skills, supporting greater retention and progression outcomes.

Equal and fair remuneration

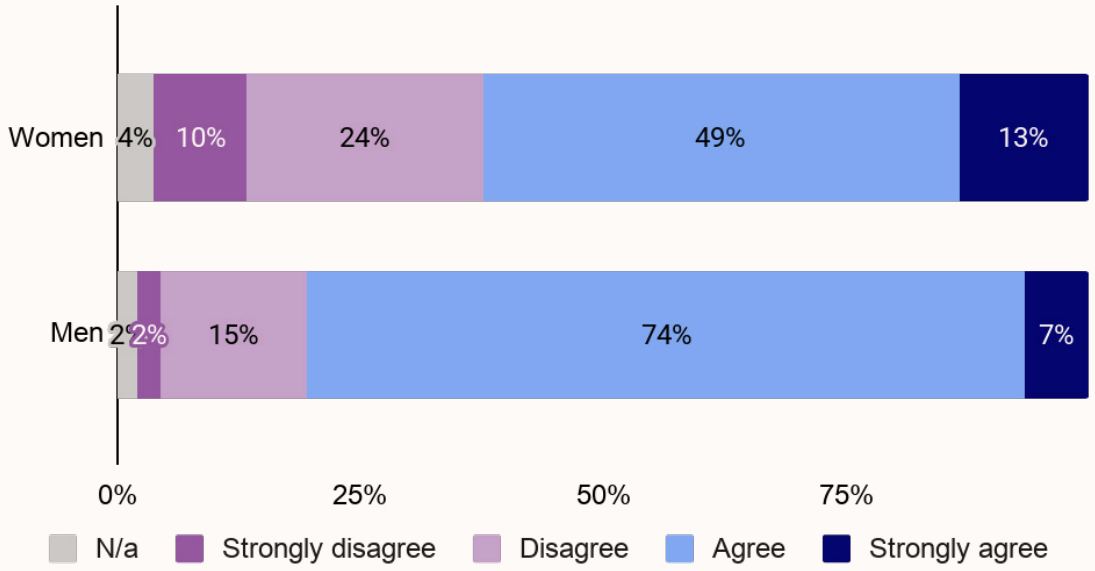
> "Having transparent pay and promotions would go a long way in exposing and addressing bias, and ensure decisions are based on merit not subjective judgements. I think it would build trust and fairness and make it more likely talented women will stay, grow and develop into leaders."

The survey interrogated perceptions of fairness in pay remuneration. For women, views are notably mixed. While a majority lean positive, with 62 per cent agreeing that their initial pay offers were fair, this still leaves more than one third expressing doubts or dissatisfaction. This suggests a sizable group of women feel disadvantaged or undervalued when entering cyber security, a situation that may have long-term implications for equity and progression. We recommend future research explore whether this feeling at entry is linked to workplace cultures and gender pay gap data.

For men, perceptions are considerably more positive. A striking 81 per cent of men agreed that their initial pay offers were fair (see Figure 20). Only 17 per cent disagreed or strongly disagreed.

Qualitative feedback shows that this divergence stems from women being more likely to perceive a lack of pay transparency and equity. For example, one respondent noted that they were paid differently compared to their peers with similar roles and experiences. Others advocated that 'Transparent promotion and pay practices is really important in helping women advocate for themselves and reduce the gender pay gap'.

Figure 20. Perceptions on fairness of initial pay remuneration, by gender



Source: Cyber 5050 survey. Respondents (n=214) were asked 'To what extent do you agree or disagree with the statement that ''Initial pay or remuneration offers are fair".

Inclusive workplace cultures

> "Culture is important, not things like standalone gender equity training. If the culture is good, poor behaviour is simply not tolerated."

Survey respondents highlighted that proactively fostering an inclusive workplace culture was key to retaining a gender diverse workforce. Many described an inclusive culture as a preventative measure to microaggressions and poor workplace experiences.

Respondents suggested implementing initiatives that could strengthen workplace relationships, creating social spaces where different interests and communication styles are welcomed and prioritising cultural safety for women from diverse backgrounds to foster greater belonging and inclusion across the workforce.

Several respondents noted that organisational commitment to gender equality can also make a difference in encouraging employees to feel valued and pleased with their workplace, with one sharing 'I felt well supported and encouraged based on my gender'.

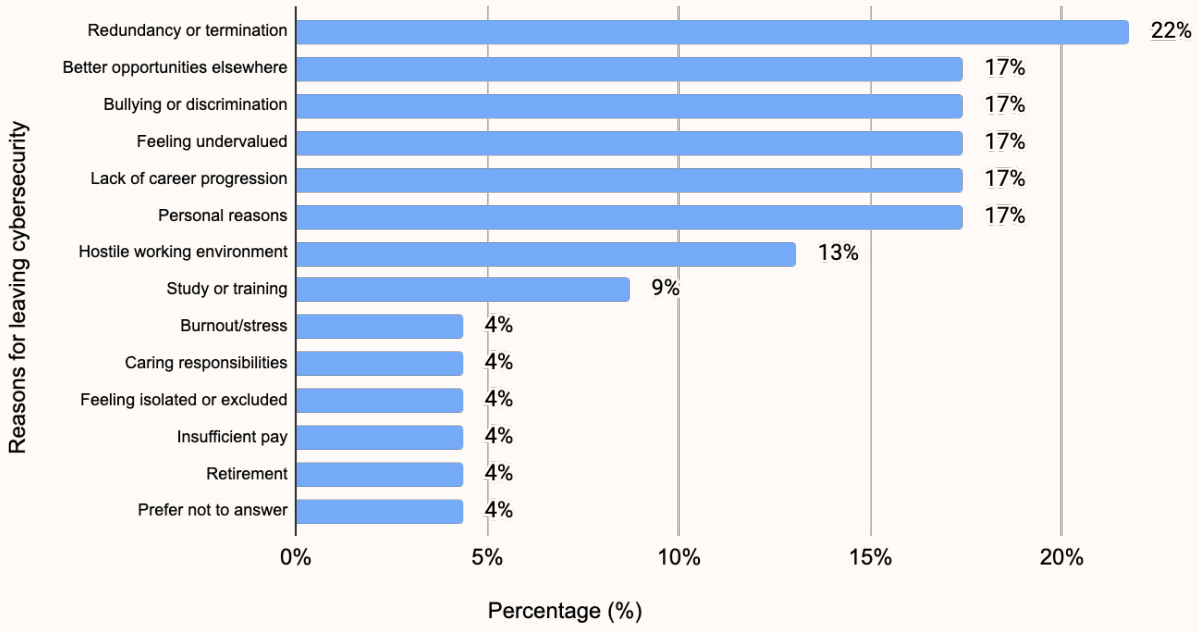
> "That said, I have also had the privilege of working with strong allies - people who notice and recognise the microaggressions that I face, who openly validate my skills, and who have made a real effort to include and support me. Their encouragement and recognition have made a tangible difference, and helped me feel valued and seen, and excited to come to work despite some of the issues I've experienced."

Men's support plays a critical role in improving workplace culture. Many respondents reflected that positive experiences of receiving support from male colleagues had prevented them from leaving the industry. One respondent shared that 'if it wasn't for a handful of very supportive male leaders, I'd have given up by now', demonstrating the powerful impact of positive leaders and strong supporters. This indicates that increased visibility of male supporters and gender inclusivity training to build men's support could encourage greater retention of gender diverse workforces.

Understanding reasons for leaving

We received 23 responses from people who had left cyber security. Figure 21 shows the most cited reason was redundancy or termination, suggesting organisational decisions rather than personal choice played a significant role in workforce exits. A hostile working environment was a notable factor, cited by 13 per cent of respondents, highlighting cultural or organisational problems.

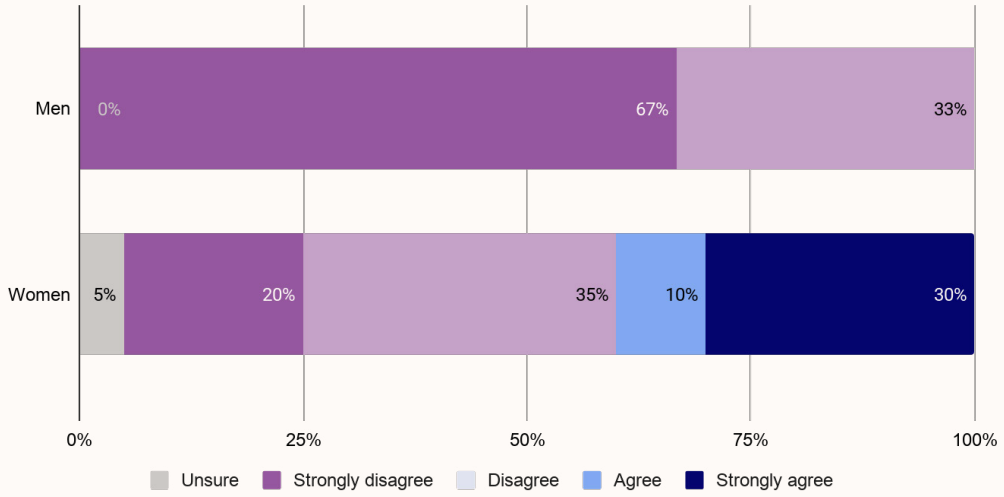
Figure 21. Reasons for leaving cyber security



Source: Cyber 5050 survey. Respondents who previously worked in cybersecurity (n=23) were asked 'What is the primary reason you no longer work in cyber security?'

Of those who left cyber security, 40 per cent of women agreed that their gender contributed to their decision to leave the industry.

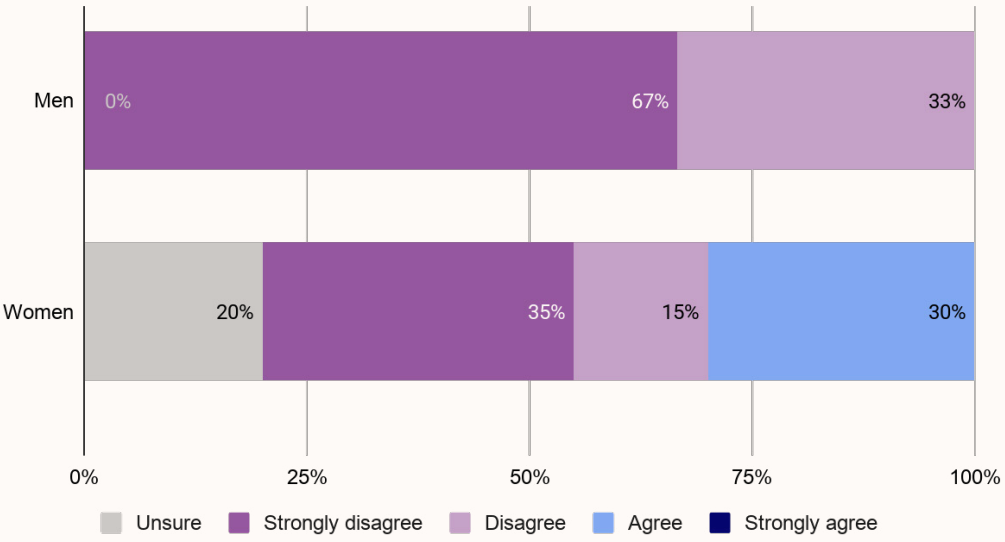
Figure 22. Extent to which gender contributed to the decision to leave cyber security



Source: Cyber 5050 survey. Respondents who previously worked in cybersecurity (n=23) were asked 'To what extent do you agree or disagree' about the statement 'My gender contributed to my decision to leave cyber security'. Of these respondents, n=20 identified as women or female and n=3 identified as men or male.

Additionally, the majority of men and half of the women respondents who left cyber security did not feel supported when they left their job. Men reported feeling less supported than women, with more than two thirds (67%) strongly disagreeing that 'I felt supported when I left my cyber security job', compared to 35 per cent of women (see Figure 23).

Figure 23. Extent to which respondents felt supported when they left cyber security



Source: Cyber 5050 survey. Respondents who previously worked in cybersecurity (n=23) were asked 'To what extent do you agree or disagree' about the statement 'I felt supported when I left my cyber security job'. Of these respondents, n=20 identified as women or female and n=3 identified as men or male.

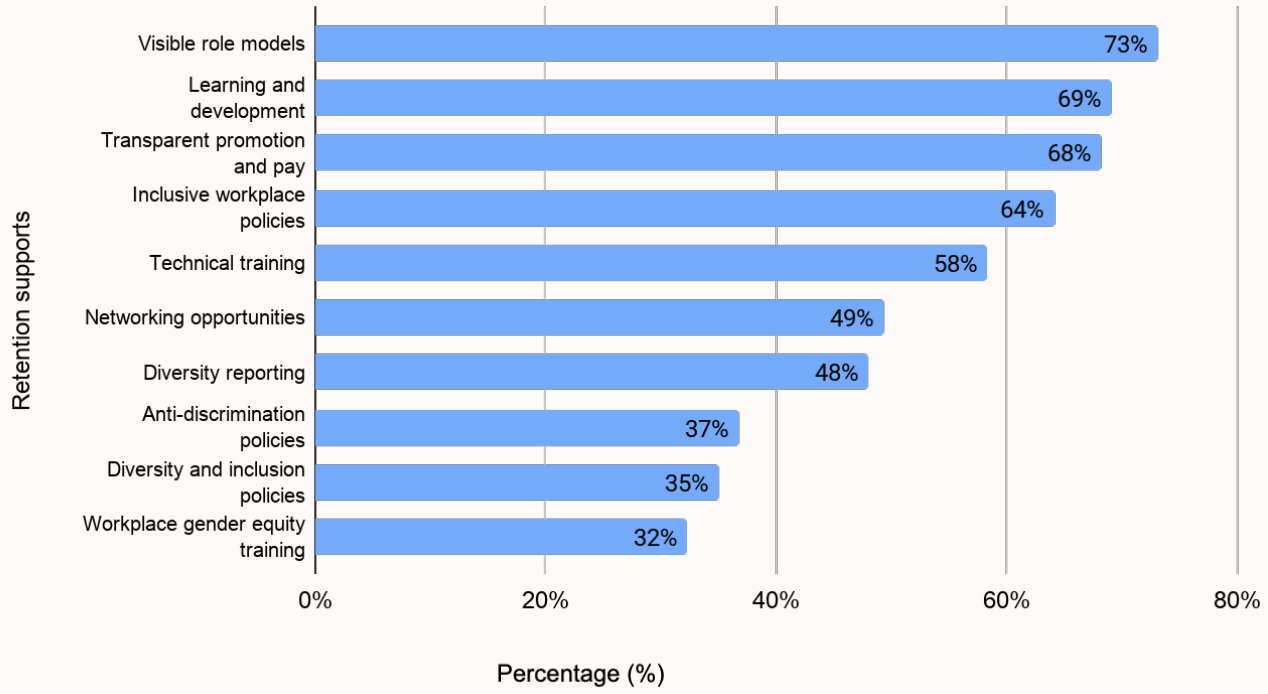
Supports for retention and progression

Figure 24 displays the most valued supports for retention and progression for both women and men combined. All emphasise visibility, fairness, and professional growth. The most highly valued support, identified by 73 per cent of respondents, is the presence of visible role models in cyber security. This reinforces findings that demonstrate the importance of representation and mentorship in fostering belonging.

Transparent promotion and pay practices were also seen as crucial, with 68 per cent of respondents agreeing. This reinforces earlier findings that women often question the fairness of initial remuneration and progression processes. Other strongly endorsed supports include inclusive workplace policies such as flexible work and paid parental leave (64%) and technical training (58%). These responses reflect a desire for workplaces to not only provide professional growth but also accommodate different life circumstances. Networking opportunities were also valued by 49 per cent of respondents, indicating the importance of professional connections and peer support.

Responses suggested that while workplace training has a role to play in improving retention and progression, structural or cultural changes are viewed as more impactful.

Figure 24. Supports for retention and progression

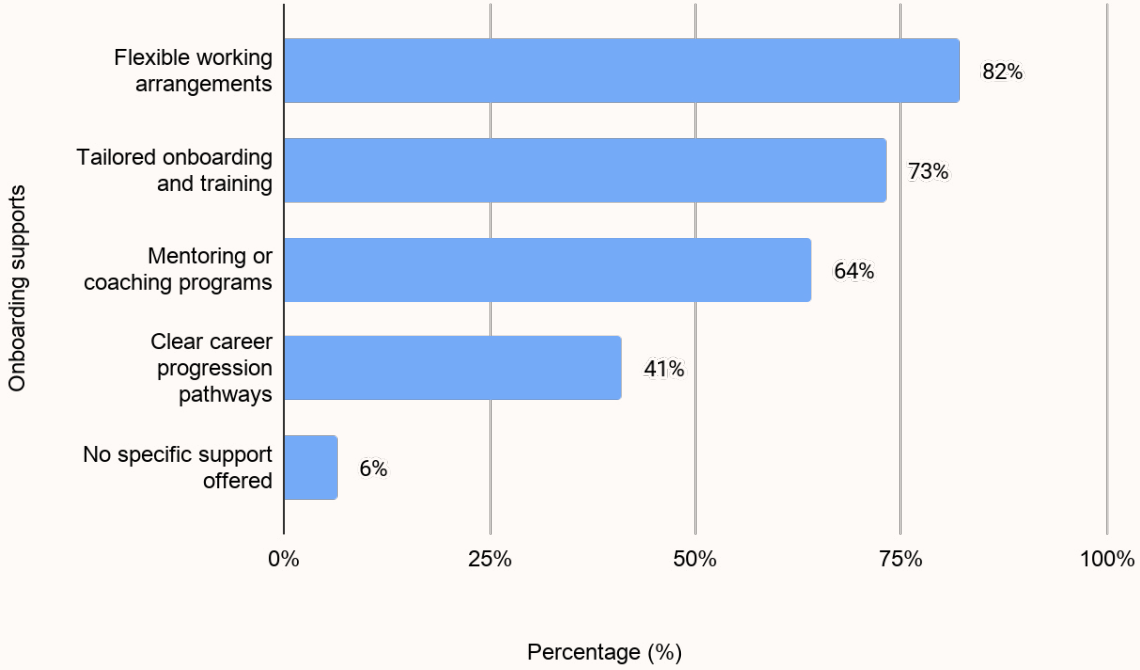


Source: Cyber 5050 survey. Respondents who currently and previously worked in cybersecurity (n=223) were asked 'Which of the following do you think would support retention for women and gender diverse people in cyber security?'.

We received responses from 78 hiring managers. Figure 25 shows the most commonly provided support organisations offer to new hires is flexible working arrangements, reported by 82 per cent of hiring managers. While this reflects the flexible arrangements viewed as adequate by hiring managers, this may not reflect the flexible work arrangements sought by all employees.

This is followed by tailored onboarding and training (73%) and mentoring or coaching programs (64%), both of which highlight the emphasis on helping employees adapt to their roles and build confidence. Only 41 per cent of hiring managers report offering clear career progression pathways, suggesting that while initial training and support are common, long-term development and advancement structures are not prioritised.

Figure 25. Types of onboarding supports provided



Source: Cyber 5050 survey. Hiring managers (n=78) were asked 'What support does your organisation provide to candidates after they are hired?'.

Key findings

- The visibility of gender diverse role models is a critical element to retain women in cyber security.
- Women are less likely to experience positive career progression opportunities compared to men, and opportunities for leadership training, mentorship and fair and transparent remuneration practices are also necessary.
- However, increasing opportunities alone is not enough to retain talent. Culture change is also crucial. Inclusive leadership and men's support are key factors to initiate sustained and meaningful culture change.
- The most commonly reported reason why individuals left cyber security was due to redundancy or termination. However, bullying, lack of career progression, feeling undervalued and opportunities in other industries are the most common reasons individuals chose to leave cyber security.
- Women were more likely to agree that their gender contributed to their decision to leave, however men felt less supported than women when they left cyber security.

4. RECOMMENDATIONS

Significant cultural change is required to improve gender equity in cyber security. FW and Australian Women in Security Network make 11 recommendations to help organisations take action now. Recognising that cultural change takes time and concerted effort, we also make four recommendations for organisations to implement over the longer term.

These recommendations are based on the findings of the report, as well as FW and Australian Women in Security Network's understanding of best practice for the inclusion of women in cyber security. These recommendations align with broader existing research about gender inclusion in male-dominated industries. They are designed to support organisations reap the well-established business benefits of a gender balanced workforce, as well as meet the skills and labour demand in an area critical to national security.

The cyber security industry is not alone in the challenges it faces. Cultural and systems change is difficult. However, cyber security is also an area with significant opportunities, and these recommendations will enable cyber workplaces to grow and change.

Actions to take now

Recommendation 1

Take a zero-tolerance approach to microaggressions

Invest in training to address microaggressions: Invest in training that specifically addresses all forms of microaggression, whether they be driven by gender, race, age or any other misconception.

Provide immediate support for those experiencing and severely impacted by microaggressions: Encourage and support the victim to seek advice or counselling through the organisation's Employee Assistance Program, an employee resource group or external work health and safety or mental health services.

Develop a policy and/or guidelines on microaggressions: Implement clear policy and/or guidelines to establish what is permissible in the workplace, as well as to outline potential consequences.

Encourage people to report microaggressions: Encourage people experiencing or witnessing microaggressions by identifying and encouraging them to report incidents through appropriate and safe channels such as their direct line manager or People and Culture team. Ensure all reports are addressed through fair, thorough, and unbiased investigations, treating those who report incidents with respect, confidentiality and empathy throughout the process and protecting them from any adverse consequences.

Recommendation 2

Take a zero-tolerance approach to bullying and sexual harassment

Model standards of behaviour: Encourage cyber security leaders to be proactive and vocal about expected standards of behaviour in their teams and departments, communicating widely and regularly with all employees. Embed conversations about sexual harassment in routine conversations, such as executive, staff and team meetings.

Prioritise accountability: Take a zero-tolerance approach to bullying and sexual harassment, prioritising accountability for incidents and ensuring consequences are visibily enforced.

Review and update existing policies: Implement annual reminders to review existing workplace policies on bullying and sexual harassment to ensure all staff understand where to report incidents and who they could go to for support.

Train managers to address bullying and sexual harassment: Equip managers with the knowledge, tools and resources to recognise incidents; handle complaints with safety, sensitivity and confidentiality; and understand when to escalate issues.

Strengthen board and workplace accountability for employee safety: Recognise reported incidents by integrating them into Occupational Health and Safety (OHS) frameworks and monitor, report and address with the same rigour as physical safety risks. This includes elevating all incidents to board and governance levels.

Recommendation 3

Address excessive workload and burnout

Monitor workloads and additional hours: Require senior managers and leaders to proactively monitor the number of additional hours staff are working and prioritise the reduction of hours where possible.

Plan for high-intensity periods: Create plans to manage high-intensity workload periods in advance to mitigate burnout. This can support teams to develop innovative ways to gain efficiencies.

Recognise additional hours: Break existing cultures of constant additional hours, requiring employees, regardless of rank or seniority, to take time-in-lieu and/or time off.

Recommendation 4
Commit to inclusive marketing and job ads

Use inclusive language in job ads: Review and embed inclusive language across all job advertisements. This includes removing gender-coded language, highlighting flexible working opportunities, and developing criteria that recognise transferable and non-technical skills. In addition, be conscious of the imagery used in recruitment campaigns.

Market cyber security differently: Avoid reinforcing existing industry and/or gender stereotypes. Instead, promote the breadth of industry benefits, including that roles are in demand, secure and well-paid. Consider highlighting benefits of the role that may appeal to women, such as a sense of purpose.

Recommendation 5
Invest in inclusive recruitment

Review and strengthen existing recruitment processes: Assess and identify areas to strengthen existing recruitment practices in line with the Department of Home Affairs' Inclusive Cyber Security Recruitment guide.[36]

Train recruiters to reduce bias: Invest in unconscious bias training for hiring managers and recruiters to prevent bias in hiring decisions. Ensure recruiters hiring for technical roles have a foundational understanding of the technical and transferable skills required for a role to mitigate an over-emphasis on technical skills.

Require gender-inclusive recruitment panels: Implement gender-balanced recruitment panels to encourage psychological safety for female candidates and demonstrate the organisation's commitment to gender equitable recruitment.

Reevaluate interview requirements: Consider providing interview questions in advance to reduce performance anxiety and allow candidates to better articulate their strengths and value to the role. Shift the focus from a binary understanding of technology use and technical skills to an understanding of competencies and transferable skills.

Avoid individual and/or token hires: Consider hiring multiple women candidates simultaneously. This approach ensures that women entering cyber security have access to peer support and are less likely to be isolated.

[36] Department of Home Affairs (2025).

Recommendation 6
Create opportunities for progression

Promote opportunities internally: Advertise cyber roles internally with a focus on transferable skills, which is likely to increase not only the quality of candidates but also the number of women entering cyber security.

Create shadowing opportunities: Promote shadowing opportunities for technical roles across teams to enable more women and gender diverse people in non-technical roles to upskill in technical areas that interest them.

Require succession planning: Embed clear and transparent succession planning in all teams. This means thinking strategically about future roles, identifying women employees with potential, and proactively supporting them to build the skills required to take on those roles once they become vacant. Organisations should communicate their commitment to succession planning widely, and ensure women who have been identified for their future potential are aware of this.

Invest in women employees: Develop formal mentorship programs to support women's leadership development, particularly for those wanting to build skills and knowledge across different cyber security roles. Encourage and sponsor more women and gender diverse people into accelerator programs to enhance their skills and build their leadership potential.

Recommendation 7
Maintain and expand flexible work opportunities

Educate leaders on the business value of flexible work: Ensure people managers understand the benefits of flexibility, how to make it work in practice, and how they can support employees to utilise these arrangements.

Create part-time and/or job-share roles: Develop innovative ways to enable flexible work for high-risk and/or on-call roles with traditionally limited access to flexible work. For example, consider enabling job sharing during specific work hours such as during school pick up to allow more women to balance caregiving responsibilities without facing consequences on their career.

Frame flexible work in light of business and individual benefits: Avoid framing flexible work and parental leave as policies that support women only. Promote the benefits of men utilising these entitlements.

Actions to plan for

Recommendation 8

Commit to culture change from the top

Understand your cyber employees: Implement an organisation-wide or cyber security department-wide employee satisfaction survey to ensure senior leaders can identify, monitor and address key cultural or wellbeing issues.

Develop metrics of success: Define and communicate the equity goals your organisation is trying to achieve. For example, 40:40:20 leadership targets are being adopted across Australian industries, alongside public commitments to closing gender pay gaps. Report progress towards these targets regularly to executive teams and boards.

Recognise inclusive leadership as a core competency: Celebrate inclusive leadership at all levels of your organisation. Where appropriate, include KPIs and targets for all people managers at all levels.

Invest in ongoing development and training: Ensure the business case for investing in gender equality is well understood by all leaders, including people managers, executive teams and boards.

Recommendation 9

Engage men as agents of change

Support men to create change: Engage men as advocates, mentors and sponsors, as they are more likely to create a safe and inclusive workplace for all.

Explain the benefits of equity to all: Make a public commitment to gender equity, and provide regular, ongoing communications about the benefits of gender equity for everyone, regardless of gender.

Recommendation 10

Report on gender leadership and pay gaps

Monitor and report key metrics: Track changes in the composition of the leadership workforce over time and address areas facing particular gaps in gender diversity. Implement annual monitoring and reporting to track changes on the leadership composition of your organisation or department. Additionally, organisations are strongly encouraged to review and report on gender pay gap data to ensure equal and fair remuneration for all genders.

Recommendation 11
Build long-term pipelines

Invest in paid pathways into the profession: Expand placements in existing programs and prioritise entry for those who have taken career breaks or have transferable skills from other industries.

Engage with untapped talent: Engage with work-ready pools of untapped talent from other industries. For example, women in industries and occupations with transferable knowledge and/or skill sets and women who have been outside of the paid workforce for an extended period, but are looking to return.

APPENDIX: OUR APPROACH

Survey and consultation

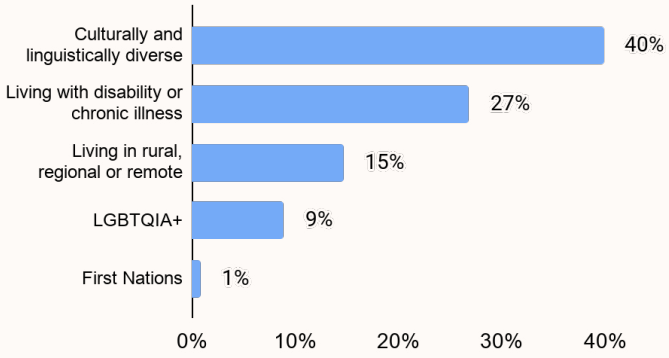
This report is based on data collected between 9 July 2025 and 25 August 2025. We analysed 346 responses from individuals who currently work in, previously worked in, or aspires to work in cyber security in Australia using an online survey tool, Survey Monkey.

We included 3 responses from New Zealand. In addition, we received 117 incomplete and 15 disqualified responses, which were excluded from our analysis. This represents a 72 per cent survey completion rate, exceeding survey benchmarks.

Of the 346 completed responses, 80 per cent (n=278) were women, 15 per cent were men (n=53) and 1 per cent (n=4) identified as gender diverse. In addition, one per cent of respondents (n=2) preferred using a different term to describe their gender and one per cent (n=9) preferred not to answer. Due to the small sample of gender diverse respondents who currently work in cyber security (n=1), we excluded this response from gendered analysis. However, responses from non-binary individuals were incorporated in all qualitative feedback and non-gendered quantitative analysis.

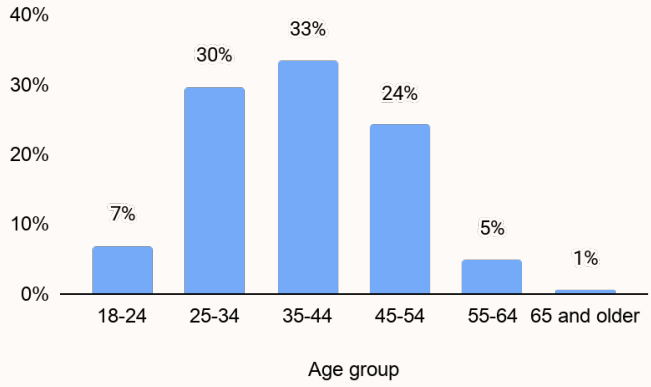
Respondents were segmented into three groups based on their responses. This included:

Figure 26. Diversity of respondents



Source: Cyber5050 survey.

Figure 27. Age group of respondents



Respondents varied across age ranges, a vast majority (94%) being under 55 years of age.

- Individuals currently employed in cyber security (n=200)
- Individuals who were previously employed in cyber security (n=23)
- Individuals who aspire to work in cyber security (n=123)

We also held an in-person opt-in consultation on 1 August 2025 at the AWSN Summit. 31 attendees of all genders joined the session.

We used online qualitative analysis software, Delve, to analyse free-text survey responses and consultation feedback.[37] We took a deductive approach to thematic analysis, shaped by the core aims of the research, which are to understand the specific barriers to the entry, retention and progression of women and gender diverse people in cyber security in Australia.

Note on terminology

When analysing qualitative free-text responses, we used the following terminology.

- 'Many' to group eight or more responses
- 'Some' or 'several' to indicate five to seven responses
- 'Few' to specify three to four responses
- 'A couple' to indicate two responses.

Statement on AI

Our research team used Google Gemini to identify grammatical errors and rephrase sentences for conciseness. Our team also used Delve's AI chat feature for qualitative data analysis assistance, including theming quotes and summarising snippets.

Throughout the research process researchers maintained critical oversight, thoroughly critiquing AI-generated information to ensure accuracy and address potential bias. No AI tool was used to write this report.

[37] Twenty to Nine LLC (2024).

REFERENCES

Australian Cyber Security Centre (2022). Annual Cyber Threat Report July 2021 –June 2022.
https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf

Australian Trade and Investment Commission (2025). No codes cracked: Australia's drive to invest in new cyber technology. Australian Trade and Investment Commission.
https://international.austrade.gov.au/en/news-and-analysis/news/no-codes-cracked-australias-drive-to-invest-in-new-cyber-technology

Beyond Blue (2025). Burnout.
https://www.beyondblue.org.au/mental-health/work/burnout

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

Canberra Cyber Hub (2025). More women are signing up for careers in cyber security.
https://canberracyberhub.com.au/news-and-events/more-women-are-signing-careers-cyber-security

Cybersecurity Ventures (2023). Women to hold 30 per cent of cyber security jobs globally by 2025.
https://cybersecurityventures.com/women-in-cybersecurity-report-2023/

Deloitte (2025). Gen Z and Millennial Study - Growth and the pursuit of money, meaning and well-being.
https://www.deloitte.com/content/dam/assets-shared/docs/campaigns/2025/2025-genz-millennial-survey.pdf

Department of Home Affairs (2023). Australian Cyber Security Strategy 2023-2030.
http://homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

Department of Home Affairs (2025). Inclusive Cyber Security Recruitment.
https://www.homeaffairs.gov.au/cyber-security-subsite/files/inclusive-cyber-security-recruitment.pdf

Department of the Prime Minister and Cabinet, Public Service Research Group and Australian Centre for Cyber Security (2017). Women in Cyber Security Literature Review. UNSW Canberra.
https://unsw.adfa.edu.au/sites/default/files/documents/Cyber-Security-Literature-Review.pdf

Department of the Prime Minister and Cabinet (2023). Attracting a diverse cyber security workforce. Lessons from an analysis of Australian job ads.
https://www.pmc.gov.au/sites/default/files/2025-06/attracting-diverse-cyber-security-workforce.pdf

Department of Employment and Workplace Relations (2025). There's job security in cyber security, Your Career.
https://www.yourcareer.gov.au/resources/articles/job-security-in-cyber-security

Gartner, R. E. (2022). A New Gender Microaggressions Taxonomy for Undergraduate Women on College Campuses: A Qualitative Examination. Violence Against Women. https://pmc.ncbi.nlm.nih.gov/articles/PMC8529990/#:~:text=Gender%20microaggressions%20are%20everyday%20slights,women%20is%20normative%20and%20permissible.

Kalla, M. (2023) What are microaggressions? And how can they affect our health?. *The Conversation*. https://theconversation.com/what-are-microaggressions-and-how-can-they-affect-our-health-193309

RMIT University (2023). Improving Gender Representation in Australia's Cyber Security Workforce. https://www.rmit.edu.au/research/impact/improving-gender-representation-in-cyber-security-workforce

RMIT University (2024). Investigating the Reasons Why Women Leave the Cyber Security Workforce and Strategies to Address this Attrition. Policy Paper. https://www.rmit.edu.au/news/ccsri/understanding-gender-dimensions-project-study

RMIT Centre for Cyber Security Research and Innovation (2025). Five Year Impact Report. https://www.mruni.eu/wp-content/uploads/2025/09/RMIT-Impact-Report-Digital-1.pdf

Sanders et al. (2015). The power of flexibility: A key enabler to boost gender parity and employee engagement. Bain and Company. https://media.bain.com/Images/BAIN_REPORT_The_power_of_flexibility_Boosting_gender_parity.pdf

Swinburne Open Ed (2025). Is cyber security a good career in Australia? How to get started. https://www.swinburneopen.edu.au/explored/careers/is-cyber-security-good-career-path-australia

Twenty to Nine LLC (2024). Delve Online Qualitative Data Analysis Software. Qualitative Data Analysis Software. http://www.delvetool.com

University of New South Wales (UNSW) (2025). How to become a cyber security analyst. https://studyonline.unsw.edu.au/blog/how-become-cyber-security-analyst

Workplace Gender Equality Agency (2025). Gender Equality and Caring. https://www.wgea.gov.au/gender-equality-and-caring.

Workplace Gender Equality Agency (2026). What is the gender pay gap? https://www.wgea.gov.au/the-gender-pay-gap

Cyber5050

CyberCX

awsn
Australian Women in Security Network

Canberra Institute of Technology

Australian Services Union
By your side