

Women in Security

Preliminary Insights Report

4 March 2022

RMIT Centre for Cyber Security Research and Innovation

Prepared for the Australian Women Security Network

Acknowledgment of Country

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

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

Executive Summary

At the same time that Australia's security sector is growing in importance, it is widely observed that it suffers from a skill crisis and a distinct lack of diversity, particularly when it comes to women's participation. This is not only indicative of the inequitable biases and barriers that impede women's career opportunities and progression in the sector. The under-representation of women also suggests that the sector is not operating as optimally as it could, given the growing evidence that a more diverse workforce brings greater innovative potential, strategic intellect and problem-solving capacity.

The Australian Women in Security Network (AWSN) is committed to improving women's representation in the sector. However, to measure the impact of the AWSN's initiatives, it needs a baseline picture. Currently **there** is no **robust available** measure of the gender composition of Australia's security industry **or a clear picture of the types of jobs that women are undertaking. Looking specifically at the cybersecurity workforce as a part of the broader security sector**, available estimates suggest that women comprise between 11% and 24% of the cybersecurity workforce, meaning that women currently constitute a stark minority.

This report outlines the insights from existing literature, and the survey proposal design, that will equip AWSN to make an impact in attracting and retaining more women in the security sector, including cybersecurity. This investment will provide AWSN with accurate baseline data to measure the effectiveness of their intervention programs and track changes in women's participation in the industry over time.

The first key goal of this study is to gain an accurate picture of the number of women in security and the types of roles they are undertaking. The second key goal is to gain deeper understanding of the factors that support women's involvement in the sector as well as the barriers that impede women's careers. These insights will help inform the AWSN to invest in preventions that will help attract, manage and retain women in the industry. The overarching objective of this study is how to systematically expand the sector's talent pool to best equip it for the growing challenges and demands it faces.

Contents

| | |
|-------------------------------------------------------------------------|----|
| Executive Summary | 3 |
| 1. Why is this study needed? | 5 |
| 2. Scope and focus of this study | 8 |
| 2.1 Size and significance of the sector | 8 |
| 2.2 Distinguishing between Information security and Cybersecurity | 9 |
| 2.3 Looking through the lens of people: global skill crisis | 10 |
| 2.4 Looking through the lens of diversity | 11 |
| 3. Delving into the crux of the issue | 13 |
| 4. Next steps | 16 |
| 5. Bibliography | 17 |
| 6. About the authors | 20 |

1. Why is this study needed?

“Our estimation is that we, in Australia, need 8000 more practitioners to meet status quo by 2025, and 10,000 to 11,000 to deal with growth of more than one million globally.”

Professor Jill Slay, SmartSat CRC Chair of Cyber Security and President/Chair of Australian Women in Security Network (2021).

The expanding importance of the security sector across the economy, combined with an increasing awareness of the value of diversity and inclusive representation in professional contexts, points towards the need to examine the gender composition of the security industry. In particular, the gender composition of the security workforce requires concerted focus given existing indication that women are largely under-represented.

There is no comprehensive data that reliably measures the gender representation of the Australian security workforce or describes the types of roles that women in the sector undertake. Available studies over the years indicate that the women working in cyber security vary between 11% (Reed et al., 2017; Williamson et al., 2017) to 24% (ISC², 2018) globally, with no specific Australian empirical research being undertaken.

The under-representation of women in the security sector is similar to the dynamics observed other traditionally male-concentrated fields, such as construction, mining, automotive industries, and in the STEM fields (Science, Technology, Engineering and Mathematics) more broadly. This implies that, to some extent, the factors that explain women’s under-representation in the security sector, including especially at senior levels, will be similar to the factors that have been identified as barriers and biases to women in these other fields.

These factors include workforce culture and practices that perpetuate unconscious bias and gender norms that constrain women; a lack of female role models and opportunities for females to form professional connections and access career-relevant information; an impression created by stereotypical images that women do not “belong” in the field; and the

perception among women that the field does not offer equitable opportunities and the fulfillment of the career aspirations that women are seeking. Additionally, it is also possible that the security industry presents further biases and barriers that distinguish it from other male-concentrated fields, which this study seeks to uncover.

There is a need to accurately understand the factors that can either support or deter women from pursuing, and flourishing in, a career in the security sector. This is not just a matter of addressing inequalities of opportunity for women at an individual level. There is also a need for the industry to understand how it is falling short of achieving its optimal performance, and fully meeting the needs of the client base it is responsible for servicing, if it is not operating with a gender balanced composition and is failing to attract, nurture and retain the full breadth of talent, skills and the innovative capacity that is potentially available within the workforce

The Australian Women Security Network (AWSN) was founded in 2014 as an open and inclusive network of like-minded people to grow, retain and empower women in the security community within Australia. It provides opportunities for women to connect and support each other professionally in a male dominated occupation. To ensure the Australian Women in Security Network (AWSN) is making an impact on attracting and retaining women in the security industry, baseline data and insights into experiences of women involved in the sector are needed. This information can help to guide AWSN in its design of intervention programs and to track its programs' success, supporting AWSN to grow and make a meaningful difference as the industry's key representative organisation for women.

This study is the first independent analysis specifically focussed on the Australian security workforce including protective security, security governance, information security, physical security, and personnel security. The baseline data collated by the study will allow for future longitudinal studies of the Australian security industry, including studies to better understand the career trajectories of workers and changes in the gender composition of the sector.

The survey data and insights will inform Australia's industry and government in policy, workforce planning and capability development. AWSN will use the insights from the study as a baseline on which to measure the success of its programs.

Throughout this study, the binary classification of gender is primarily used because this has been the predominant way that data has been collated and analyses have been conducted in the past. This study emphasises that understanding the experiences of individuals who identify across the gender spectrum, and appreciating the way that gender intersects with other dimensions of personal identity and lived experiences (such as cultural background, socioeconomic background, disability, Indigenous status, and English language proficiency) are important consideration for ongoing research and analysis.

The products, services and information provided by security industry – broadly defined – plays an essential role in the operation of businesses and governments. The industry provides important infrastructure to the wider economy and impacts how households manage their everyday lives.

2. Scope and focus of this study

The Australian Government Attorney Generals department uses the umbrella term ‘protective security’ to encompass the Australian security industries and their roles. Protective security is partitioned into four sectors: information security, personnel security, physical security and Security governance (Protective Security Policy Framework, n.d.). The AWSN has members which cover all four of these industry sectors.

Information security and Security governance are relatively new fields, which do not have any required professional accreditation in Australia. Physical security on the other hand is regulated by licensing and personnel security (at least for government jobs, and contractors) requires formal security vetting. Each of the sectors of protective security have different skills, training pathways and career possibilities, yet they are all drawn together by a desire to protect

2.1 Size and significance of the sector

One of the major results from the massive expansion of globalisation is the fast grow of the security industry. The private security services market is valued at US\$85 billion worldwide, with an annual growth rate of between 6% to 8% (Williams and Abrahamsen, 2022). As a result, the provision of security services has experienced significant transformation (Hansen, Loftus and Loader, 2016). This has brought large organisational challenges, such as the difficulty of find suitably qualified people to fill available roles (Cropper, 2021).

Despite the growth of this industry, and its associated recruitment challenges, scholarly attention has been mainly focused on features of the industry, such as “the role of mercenaries and private military companies” (Williams and Abrahamsen, 2022: 01). Other aspects, such as the representation of women in the provision of security services, have received considerably less empirical and theoretical analysis (Davies, 2017). This study’s analyses aims to assist in alleviating current workforce challenges.

2.2 Distinguishing between Information security and Cybersecurity

As an information-centric society, the securing of information for information communication technologies (ICT) and their users has become of principal importance for organisations, it becomes important to differentiate different terminologies. As a generic terminology used, ICT covers information security solution, and management which involves processes, technology and people aspects (Reid and Van Niekerk, 2014). The last aspect is crucial for the appropriate use of technologies in a secure manner to ensure that the process aspect is protected (Reid and Van Niekerk, 2014). Due to this, the concept of culture of information security was developed (Thomson, von Solms, and Louw, 2006; von Solms, 2000), which covers aspects related to socio-cultural measures, supporting technical security methods (Schlienger and Teufel, 2003).

As organisations continue to be more information-oriented, they are exposed to risks and threats to their information and users of ICT require awareness of cyber security issues. To address solutions to these issues, requires a synchronized effort at national and international levels, involving governments and the private sector (Reid and Van Niekerk, 2014). The private security services market is valued at US\$ 85 billion world-wide, with an annual growth rate of 6-8% (Williams and Abrahamsen, 2022). As a result, the security provision continues to experience significant transformation (Hansen, Loftus and Loader, 2016), with large organisational issues such as the difficulties to find suitably and qualified people to fill available role (Cropper, 2021).

Despite the growth of this industry, and its further issues, scholarly attention has been mainly focused on aspects related to “the role of mercenaries and private military companies” (Williams and Abrahamsen, 2022: 01), when other aspects such as the impact of women in the day-to-day security services have received considerably less empirical and theoretical analysis (Davies, 2017). Results from these analyses could assist in alleviating current organisational matters.

2.3 Looking through the lens of people: global skill crisis

How secure organisations are depends on the people involved, hence, whether people use technologies, manage information and processes of information in a secure way becomes of paramount importance for organisations (Reid and Van Niekerk, 2014). Cybersecurity principally involves the protection of information, information communication technologies, preservation of the confidentiality, integrity, and availability of information in cyberspace (ISO/IEC 27032, 2012). This last concept refers to “the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form” (2012: 01). Hence, how truly secure technologies and their management are, “depend on the people involved in their use and implementation” (Reid and Van Niekerk, 2014:1). Bearing in mind the importance of information technologies and security, there is an extensive skill shortage in the industry (Smith, 2018).

Recent report suggests that around 45% of organisations are harshly lacking in this specific area of talents. Technology workers, such as cyber-security skilled talent, are approached with a new job offer once a week (Smith, 2018). This issue is worsening when acknowledging that discussion about the skills gap of cybersecurity talent “has been going on for over 10 years, and that there has been no significant progress toward a solution to this problem during the five years” (Oltsik, and Lundell, 2021: 4). This *skills crisis* has negatively impacted several organisations by increasing workload of their employees, unfilled open job requisitions, and high burnout among employees (Oltsik, and Lundell, 2021).

While research suggest ways to improve this issue, little of these recommendations advise the importance to focus on gender. In other words, one solution for the professional skills shortage of talent in this industry could be overcome by addressing the gender imbalance (Maraj et al., 2021). While women have been involved in the security field for long time, stereotypes, bias and discrimination are some of the major factors women are facing within

the security industry (Davies, 2016; Christofferson, 2018), and therefore, in the cybersecurity field (Bagchi-Sen et al., 2010; Maraj, Sutherland and Butler, 2021).

2.4 Looking through the lens of diversity

At its essence, the security industry exists to protect people, information and infrastructure: this provides stability and predictability for businesses, governments and households to go about their activities with certainty, and to invest and innovate with confidence. These are essential ingredients for a thriving economy and flourishing society. The structure of our economy – locally, nationally and globally – is evolving to place greater importance on the role of data and information. Technological change means that this data and information most commonly takes digital form, and that storage, processing, exchange and communication information takes place in a cyber forum. This process of economic transformation magnifies the importance of the cybersecurity sector.

In a parallel development to these technological and economic transformations, there has been growing awareness among both academic scholars and practitioners in the field of the value that diversity and inclusion brings to the workforce (Hewlett, Marshall and Sherbin, 2013; Rock and Grant, 2016; Turban, Wu and Zhang, 2019). In the context of cybersecurity, a workforce that is equipped with a broad spectrum of life experiences, multiple perspectives and different ways of thinking, will be better equipped to tackle the complex challenges that the sector is tasked with. Research attests that diversity within a team's composition promotes more effective problem-solving, generates more innovation and ideas, and facilitates a robust interrogation of the evidence.

The pressures and expectations placed on the cybersecurity sector intensify the value of diversity for the cybersecurity workforce. Cybercrime is transnational and the 'adversarial' personnel that the cybersecurity workforce is seeking to counter is diverse, creative and well resourced. Deepening the pool of creative talent, innovative potential, real life experiences and strategic intellect within security teams – through greater diversity and a more balanced gender composition strengthens the sector's capacity to counter security threats and

effectively protect our people, infrastructure and information. In this context, it can be clearly argued that the security industry needs women (Poster, 2018).

A barrier to diversity, however, can come in the form of inequitable opportunities and gender-patterned biases that persist in sometimes intangible ways. Insights are improving into the influence of implicit biases and barriers that are imposed on women in many vocational and professional settings, often due to the persistence of traditional practices and gender-patterned stereotypes (Gergis and Kachala, 2021). Commonly portrayed in popular culture, some clear examples of archetypes exist for the security industry: the authoritative male security guard or the lone male hacker sitting in dark rooms (often wearing a hoodie) (Larson, 2017). Similar stereotypes exist for the IT industry, which feeds into perceptions of the information and cyber security sector. Security staff depicted in fictional and news media are rarely women, a notable exception being the recent appointment of Michelle Price as CEO of AustCyber. Although some security industry events have speakers with diverse demographics (Cybercon, purplecon), many are dominated by the male archetype in their line-up of speakers and their advertising material (OWASP, Defcon, RSA). These gender-patterned dynamics impede the achievement of gender equality. An industry that does not deliver a gender balanced composition could be perceived as archaic in practice, and out of step with the contemporary values expected from its citizens.

Many people do not conform to these archetypes yet have the aptitude to work in security. Many who currently work in security do not conform the archetypes (Bachigi-Sen, 2010).

3. Delving into the crux of the issue

Women's under-representation in the sector can be considered akin to a leaky pipeline. This is an analogy that has been commonly applied to other industries experiencing gender imbalance (SAGE, 2015). Firstly, there is a need to attract women to the sector, a process that begins throughout their educational pathway and in the process of navigating their career and vocational choices relative to other fields and opportunities. Of the women who flow into the sector, there is a need to retain women throughout their career, which entails understanding the range of factors that cause women to drop out of the sector. If women drop out throughout their careers, the sector ends up with a smaller fraction of women at senior and leadership levels, having repercussions for the sector's workforce culture and its capacity to attract the next generation of women. This study's survey design is intended to reflect this leaky pipeline effect and attempt to capture the experiences of women at these various points of their career path.

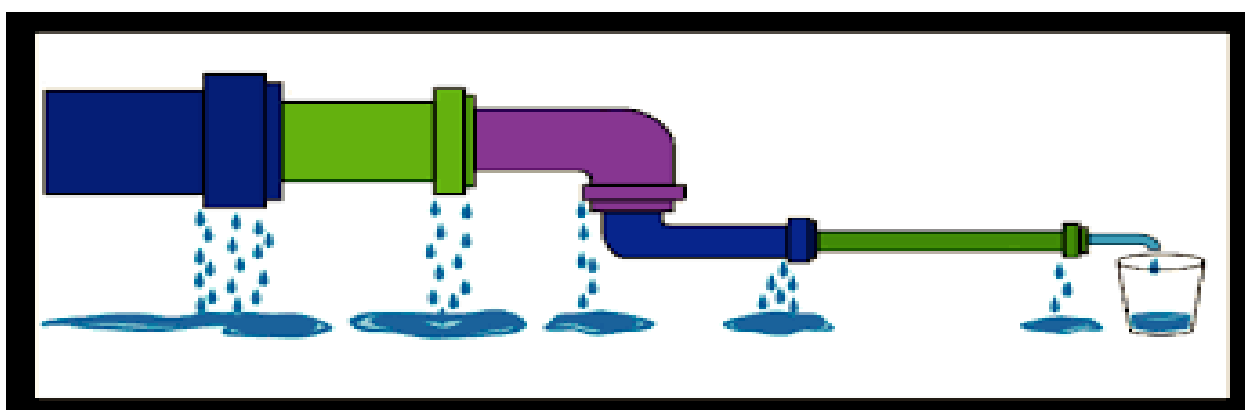


Figure1.: The Leaky pipeline (Lee, 2017)

Furthermore, existing research into gender inequalities in traditionally male-dominated sectors points towards the need for a change in workplace practices and professional culture – rather than placing the onus on individual women to correct apparent deficiencies – as the pathways to sustainable and authentic improvements (Bohnet, 2016; Fox, 2017).

This study will delve into the factors that explain women's under-representation in the sector through a direct survey of individuals involved in the sector. The following questions are proposed for survey participants:

- 1) Entry decision: What influenced your study and vocational choices? What qualifications did you attain (level and field)? What challenges did you experience while studying in these fields? Were you exposed to any role models and mentors that made a difference to your decision to enter this field or not?
- 2) Career decision: What is your current position and what are the characteristics of your employer? What is your previous position? What influenced or inspired you to pursue a career in this field? Are there any characteristics of the profession and/or workforce cultures that do you think contribute women's under-representation in the field?
- 3) Retention decision: What factors influenced your decision of whether to stay in the sector? Have you ever considered leaving the sector? If so, why? What factors affect your pace of career progression in the sector?
- 4) Management perspectives: What challenges have you experienced or observed in attracting and retaining females to the sector? What gaps in data collection do you face?
- 5) Perceptions of the value of diversity: In what ways would improving diversity of representation in the sector make a difference to the sector's outcomes, performance, and culture?
- 6) Perceptions on a sense of belonging and inclusion: Do you feel a sense of belonging to this profession?
- 7) Perceptions of workforce culture: Do you think that Australian organisations in the security sector are prepared to make cultural change to improve gender balance and inclusion in the security and cybersecurity field?
- 8) Intersectionality: Do you identify with other demographic or personal characteristics that have made a difference to your career experiences and opportunities in this field?

Drawing on the results of the survey in conjunction with other sources, the study's objectives and key issues for investigation are as follows:

- To produce an estimated number of women working in security, also computed as a gender ratio relative to men, across Australia, including with a focus on cybersecurity.
- To understand how the Australian 'cybersecurity' industry is defined and whether this is different from international definitions.
- To understand what areas of security women are participating in, including estimating what share of the women security workforce in Australia are working in cyber security technical roles.
- To understand how the Australian women's skills and capabilities can contribute to overcoming the current and future professional skills shortage in the security industry.
- To understand the enablers and barriers to women's participation in the security sector and identify practical implications arising from this research. This entails identifying how these enablers and barriers relate to broader cultural factors and institutional practices that can be shaped by changes in workplace policies and by strategic interventions by key agencies and stakeholders.
- To explore ways of creating a cybersecurity talent management system that works for women. This entails identifying the elements of a cybersecurity talent management system that would most effectively and equitably attract, select, and retain female talent, encompassing planning, employee engagement, learning and development, performance management, recruiting, onboarding, succession and retention.

4. Next steps

This Preliminary Insights Report is the first of a series that will be generated by this study. The authors bring academic rigour to their analysis of the literature and evidence, and combine this with practical insights into the operations, responsibilities and culture of the security sector and its workforce to generate actionable steps that the sector can follow to foster a more inclusive, gender balanced composition.

Through a literature review, the study will draw upon insights from existing studies of security workforce in other countries and workforce studies in Australia of similar traditionally male-dominated disciplines. Data from the Australian Bureau of Statistics, using Census data based on standardised definitions of occupations defined in the Australia New Zealand Classification of Occupations, will be used to provide empirical baselines. These insights will be benchmarked against similarly male-dominated industries, such as STEM, IT, finance and locksmithing, to generate a picture of how the security sector compares.

As the key contribution to this study, field work will be conducted that surveys current and former security industry professionals in Australia. This survey will generate a measurement of the gender composition of the sector as well as elicit responses from participants in relation to their personal experiences, perceptions and attitudes about the sector. This will generate insights into the enablers and barriers to women's participation and career progression in the sector. The intention is to survey men as well as women, so that gender-specific barriers for women can be identified.

Informed by these insights, the study will identify the practical implications arising for the sector, including systemic steps to foster a more gender equitable workforce.

As part of its process, this study will offer a standardised method of measuring the gender composition of the sector, so that this measurement process can be replicated in future years for ongoing comparability and benchmarking. This will be achieved by sharing the procedural steps that have been undertaken to conduct this study throughout the course of this report series. This information will further equip the AWSN to evaluate the success of any intervention strategies that it puts into place in pursuit of a more gender equitable workforce composition in the future.




5. Bibliography

- Bagchi-Sen, S., Rao, H.R., Upadhyaya, S. J., and Chai, S. (2010). Women in Cybersecurity: A Study of Career Advancement. *IT Professional*, 12(1), 24–31.
<https://doi.org/10.1109/MITP.2010.39>
- Berger, L., and Berger, D. (2004). *The talent management handbook*. New York.
- Bohnet, I. (2016). *What works: Gender equality by design*. Cambridge, Massachusetts: Harvard University press.
- Christofferson, D. A. (2018). *Women in security: changing the face of technology and innovation*. Springer International Publishing. <https://doi.org/10.1007/978-3-319-57795-1>
- Collings, D. G., and Mellahi, K. (2009). Strategic talent management: A review and research agenda. *Human Resource Management Review*, 19(4), 304–313.
- Cropper, S. (2021). *The Trouble With Labour: Security Industry hit hard*. Retrieved from <https://australiansecuritymagazine.com.au/the-trouble-with-labour-security-industry-hit-hard/>
- Cuberes, D., and Teignier, M. (2014). Gender inequality and economic growth: a critical review. *Journal of International Development*, 26(2), 260–276. <https://doi.org/10.1002/jid.2983>
- Cunningham, I. (2007). Talent management: making it real. *Development and Learning in Organizations*, 21(2), 4–6. <https://doi.org/10.1108/14777280710727307>.
- CyberCon <https://www.aisa.org.au/Public/Events/Conferences/Australian-Cyber-Conference-2020.aspx>
- Davies, S.J. (2017). *Women in the security profession: a practical guide for career development* (First edition.). Butterworth-Heinemann, Elsevier. Chennai, India.
<http://ebookcentral.proquest.com/lib/rmit/detail.action?docID=4689271>.
- Fox, C. (2017). *Stop Fixing Women*. Sydney: NewSouth Publishing.
- Fraze, D. (2018). Cyber Grand Challenge (CGC). Defense Advanced Research Projects Agency. Retrieved from www.darpa.mil/program/cyber-grand-challenge.
- Gergis, D. and Kachala, M. (2021). Two Ways to Improve Gender Balance in Tech, *Harvard Business Review*. <https://hbr.org/2021/12/two-ways-to-improve-gender-balance-in-tech>
- Hansen L fstrand, C., Loftus, B., and Loader, I. (2016). Doing “dirty work”: Stigma and esteem in the private security industry. *European Journal of Criminology*, 13(3), 297–314.
<https://doi.org/10.1177/1477370815615624>

- Hewlett, S.A., Marshall, M. and Sherbin, L. (2013). How Diversity Can Drive Innovation, *Harvard Business Review*. <https://hbr.org/2013/12/how-diversity-can-drive-innovation>
- Iles, P., Chuai, X., and Preece, D. (2010). Talent Management and HRM in Multinational companies in Beijing: Definitions, differences and drivers. *Journal of World Business* : JWB, 45(2), 179–189. <https://doi.org/10.1016/j.jwb.2009.09.014>
- ISC2 (2018). Women in Cybersecurity. <https://www.isc2.org/Research/Women-in-Cybersecurity#>
- ISO/IEC 27032. (2012). Information technology, security techniques, guidelines for cybersecurity. Retrieved from <https://www.iso27001security.com/html/27032.html>
- Lee, J.C. (2017). The Leaky pipeline- At what stage does one intervene, Presentation at Women in Science, Engineering, Medicine and Beyond
- Larson, S. (2017). Why do hackers always wear hoodies? Behind the stereotype <https://money.cnn.com/2017/05/26/technology/hacker-hoodie-stereotype-hacking/index.html>
- Lewis, R. E., and Heckman, R. J. (2006). Talent management: A critical review. *Human Resource Management Review*, 16(2), 139–154.
- Maraj, A., Sutherland, C., and Butler, W. (2021). Studying the Challenges and Factors Encouraging Girls in Cybersecurity: A Case Study. European Conference on Cyber Warfare and Security, 269–XIII. <https://doi.org/10.34190/EWS.21.004>
- Olsik, J. and Lundell, B. (2021). The Life and Times of Cybersecurity Professionals 2021. Volume V. Enterprise Strategy Group and the Information Systems Security Association. Retrieved from <https://www.esg-global.com/hubfs/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf>
- Poster, W.R. (2018). Cybersecurity needs women, *Nature*, p. 577-580 <https://www.nature.com/articles/d41586-018-03327-w>
- Protective Security Policy Framework (n.d.) <https://www.protectivesecurity.gov.au/>
- Reed, J., Zhong, Y., Terwoerds, L, Brocaglia, J. (2017). The 2017 Global Information Security Workforce Study: Women in Cybersecurity. Frost & Sullivan, Santa Clara.
- Reid, R., and Van Niekerk, J. (2014). From Information Security to Cyber Security Cultures. *Organizations to Societies*. Retrieved from https://digifors.cs.up.ac.za/issa/2014/Proceedings/Full/42_Paper.pdf
- Rock, D. and Grant, H. (2016). Why Diverse Teams Are Smarter, *Harvard Business Review*. <https://hbr.org/2016/11/why-diverse-teams-are-smarter>

- SAGE (2015), Athena SWAN Charter Bronze Institutional Award Handbook
<http://www.sciencegenderequity.org.au/wp-content/uploads/2015/11/SAGE-Handbook-Oct-2015.pdf>
- Schlienger, T., and Teufel, S. (2003). Information security culture - from analysis to change. *South African Computer Journal*. Suid-Afrikaanse Rekenaartydskrif, 2003(31), 46–52.
- Schmid, E.A., Pircher Verdorfer, A., and Peus, C. (2019). Shedding Light on Leaders' Self-Interest: Theory and Measurement of Exploitative Leadership. *Journal of Management*, 45(4), 1401–1433. <https://doi.org/10.1177/0149206317707810>
- Slay, J (2021). Australian Cyber Security Standards: Conceptualizing the NICE/NIST framework webinar presentation
- Smith. (2018). The intelligent solution: automation, the skills shortage and cyber-security. *Computer Fraud and Security*, 2018(8), 6–9. [https://doi.org/10.1016/S1361-3723\(18\)30073-3](https://doi.org/10.1016/S1361-3723(18)30073-3)
- Statista Research Department. (2022). *Size of the security services market worldwide from 2011 to 2020, by region*. <https://www.statista.com/statistics/323113/distribution-of-the-security-services-market-worldwide/#:~:text=The%20global%20security%20services%20market,global%20company%20or%20security%20service>
- Tarique, I., and Schuler, R. S. (2010). Global talent management: Literature review, integrative framework, and suggestions for further research. *Journal of World Business*, 45(2), 122-133.
- Turban, S., Wu, D. and Zhang, L.T. (2019). When Gender Diversity Makes Firms More Productive, *Harvard Business Review*. <https://hbr.org/2019/02/research-when-gender-diversity-makes-firms-more-productive>
- von Solms, R., and van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>.
- Warren, M and Manuel D. (2020). Australian Cybersecurity Skills and jobs NSW Study, [URL: https://www.aisa.org.au/common/Uploaded%20files/PDF/Surveys/AISA-Australian-Cyber-Security-Skills-and-Jobs-NSW-Study-2020.pdf](https://www.aisa.org.au/common/Uploaded%20files/PDF/Surveys/AISA-Australian-Cyber-Security-Skills-and-Jobs-NSW-Study-2020.pdf)

6. About the authors

| | |
|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <p>Dr Leonora Risse</p> | <p>Dr Leonora Risse is an economist with interest and expertise in gender equality in the workforce. Her research focuses on understanding gender differences in economic opportunities and outcomes, which includes understanding the gender pay gap, women's participation in the workforce, women's under-representation in leadership. She is a co-founder of the Women in Economics Network (WEN) in Australia and currently serves as the WEN National Chair.</p> |
|  <p>Dr Maria Beamond</p> | <p>Within People in Organisations or HRM (Human Resource Management), Dr Maria's Beamond research interests focus on: International HRM, corporate strategies (global talent management, corporate social responsibility, climate change), talent management, emerging economies, artificial intelligence, knowledge management, corporate organisational culture, and talent management and women.</p> <p>In addition, Maria has more than 18 years' experience working with private and government organisations.</p> |
|  <p>Dr. Joanne Hall</p> | <p>Dr Joanne Hall is a Senior Lecturer in mathematics and Cybersecurity at RMIT. With a background in abstract algebra, her research has focussed on quantum key distribution and post quantum cryptography. Her role as the internships coordinator and Program Manager for the Master of Cybersecurity degree has led to broadening her research to include cybersecurity curriculum issues and the cybersecurity needs of small business.</p> |
|  <p>Dr. Banya Barua</p> | <p>Dr. Banya Barua bridges the gap between academics and consultants. She works as a management consultant and has 20 plus years of experience working with people in human resources and strategic human resources. She specialises in leadership, leadership development and takes a special interest in women and diversity. Her research is mainly in corporate mindfulness and workplace wellbeing. She integrates her research areas with leadership and leadership development.</p> |



**Professor Matt
Warren**

Professor Matt Warren is the Director of the RMIT Centre of Cyber Security Research and Innovation and a Professor of Cyber Security at RMIT University, Australia. Professor Warren is a researcher in the areas of Cyber Security and Computer Ethics.

He has authored and co-authored over 300 books, book chapters, journal papers, and conference papers. He has received numerous grants and awards from national and international funding bodies, such as AustCyber, Australian Research Council (ARC); CyberCRC, Engineering Physical Sciences Research Council (EPSRC) in the UK; National Research Foundation in South Africa, and the European Union.



Mr Laki Kondylas

Laki Kondylas is Deputy Director, RMIT Centre for Cyber Security Research and Innovation and has a wealth of experience nationally and internationally and has held executive roles in both State and Federal Governments as well as in Academic Institutions. Laki brings a wealth of international knowledge specifically in North America where he represented Australia in Arizona, Washington DC and San Francisco.

THE RMIT CENTRE FOR CYBER SECURITY RESEARCH AND INNOVATION (CCSRI)

THE RMIT UNIVERSITY CENTRE FOR CYBER SECURITY RESEARCH AND INNOVATION (CCSRI) IS A MULTI-DISCIPLINARY RESEARCH CENTRE THAT DRAWS RESEARCHERS FROM ACROSS RMIT'S SCHOOLS AND COLLEGES TO BRING A TRULY MULTIDISCIPLINARY APPROACH TO THE ORGANISATIONAL, HUMAN AND TECHNOLOGY ASPECTS OF CYBER SECURITY.

Contact

Laki Kondylas

Deputy Director – RMIT Centre for Cyber Security Research and Innovation

Email: laki.kondylas@rmit.edu.au

Phone: 0466421933