

Cyber diversity: beyond the hoodie at the green screen



MJ Salier

Managing Associate
General Counsel &
International Regulatory

Security and trust in our online environments are key to enabling society and businesses to flourish. Good cybersecurity is a fundamental condition for conducting business internationally, as well as allowing us to safely interact with our banks and service providers online, or email confidential information with peace of mind.

Insufficient security can create distrust in these systems, leading to us missing the opportunities the digital world opens up. Diversity in cybersecurity teams drives the contribution of different perspectives, genders and backgrounds, which together create a holistic 360-degree view that is critical to the development of better security solutions.

Women currently make up less than 20%¹ of graduates from IT degrees at Australian universities - partly, I believe, due to the misconceptions about what a cybersecurity job is. The stereotype of a male in a hoodie, sitting at a green screen, working on ones and zeros in a dark room, is not only a false representation but can also create a barrier to attracting diverse talent to the field.

Women may be put off by the perceived lack of social engagement and isolation of the sector, but the reality is that Security Operation Centres (SOCs) – at least the dozens I've visited – range from modern, futuristic, high-tech centres to rooms with 10 people at computers that look just like regular offices.

The notion that technological proficiency and good communication are skills that cannot co-exist is misleading. Having said that, technically-focused experts might not always be natural people managers or have the innate ability to argue strategically and persuasively for change – this is why the industry needs people with a diverse range of skills.

Companies can invest in cross-skilling and training programs for employees to help build the workforce capability that is so important to the future of cybersecurity. Encouraging employees to work on projects with, or have placements in, cybersecurity teams can help progress this skill development with experience in real-time scenarios and activities.

Whether through formal training or secondments, cross-skilling can attract new talent to the cyber sector and help create a learning environment where everyone benefits.

In our discussion on the Counterpoint Conversations podcast, Lynwen Connick, CSO for ANZ Bank, suggested that gaining technical skills isn't as hard as people think.

Lynwen revealed she hasn't always been good at communications; it's a skill she had to learn throughout her career. Technical cyber security skills can also be learnt. Understanding even basic technical skills opens up career opportunities, particularly when paired with other skills like strategy and communication. Those who start off as coders or forensic analysts can transfer their skills and shift direction down the track.

In-house graduate programs are a very successful method to develop challenging technical skills among women in IT – particularly when paired with mentoring and sponsorship.

With female graduates generally² displaying stronger soft skills than their male counterparts – like interpersonal skills, communication skills, listening skills and time management – they often move into more managerial-focused work earlier, which means missing out on exposure to important technical skills. It is essential for graduate programs to cover technical skills for all participants, even if leadership potential is identified early on. This grounding knowledge of cybersecurity and how it works can help uncover solid career opportunities in the future.

There is a significant range of jobs and career paths within the cybersecurity industry that couldn't be further from the 'hoodie at a green screen' stereotype - and it's important we start to break down these misconceptions to help people embrace their ability to better understand technology.

Cybersecurity is an exciting, growing sector in which people strive for a secure digital world by solving complex technical and regulatory challenges every day.

Recalibrating cybersecurity to focus on the impact you can make and problems you can solve, rather than the code you can write, will go a long way to attracting more women in IT .

Companies have a responsibility to challenge stereotypes when promoting jobs in cyber. This shift in approach, combined with graduate programmes, cross-skilling and equity in employee sponsorship can create a more diverse workplace – which will ultimately help create better solutions and provide more opportunities for innovation.

-
- 1 <https://www.industry.gov.au/data-and-publications/stem-equity-monitor/university-enrolment-and-completion-in-stem-and-other-fields>
 - 2 <https://www.kornferry.com/about-us/press/new-research-shows-women-are-better-at-using-soft-skills-crucial-for-effective-leadership>