

RESEARCH INTO CYBER SECURITY ACCREDITATION IN AUSTRALIA



Table of Contents



01

Executive
Summary

02

Key
Points

03

Key
Problems

04

Key Findings

17

About AISA

18

Acknowledgements

Executive Summary



Research into Cyber Security Accreditation in Australia

The Australian Information Security Association (AISA) undertook a study across over 9,500 cyber security members to investigate accreditation (licensing or professionalisation as it may also be known) of the sector in Australia.

AISA acknowledges that a holistic approach is required to address market complexities and existing challenges across the industry. AISA also acknowledges that it is critical to identifying the problems such a scheme may seek to resolve before any scheme is introduced.

This paper discusses and presents findings from the research and identifies key challenges with the supply and demand side of the cyber security workforce in Australia.

The following is a summary of findings of the survey of more than 9,500 AISA members nationally. The survey was conducted in September 2022. The research output also includes data from AISA's past research investigations in 2020 and 2021.



9,500

Cyber Security Professionals









Key Points

Demand

Supply

<p>Prospective employers of cyber security professionals value the following three candidate criteria well above all others: aptitude (ability to learn), work experience and attitude</p>	<p>There is no single door of entry into the cyber security profession</p>
<p>A candidate's industry certification, education experience and background trail behind a candidate's work experience by 40 percentage points, as valued by prospective employers of cyber security professionals</p>	<p>Those who work in the profession have a diverse mix of qualifications, that may include work experience, tertiary degrees and industry certifications among other things</p>
<p>Support for industry professionalisation is mixed. Slightly more than half of respondents wanted some accreditation of the sector to ensure a base level of qualification</p>	<p>A lack of systemic or easy way to determine suitability may result in disadvantages for students as there is no mapping or labelling across all Australian tertiary providers for the different courses offered and what competencies they create</p>
<p>The strongest support for introducing accreditation came from AISA members in academia</p>	<p>Industry based certification is one method of accreditation, although nearly half of all cyber security professionals (47.6%) choose not to have them</p>
<p>Over one in four (26.4%) cyber security professionals do not want an accreditation scheme. One in five (20.5%) respondents were unsure if they wanted an accreditation scheme</p>	<p>Substantial reliance on such certificates for accreditation would disadvantage females in the workplace, since only a quarter of female cyber professionals (25.6%) have such certifications, compared to 42.4% of males</p>
<p>Over 50 industry experts and executives from Australia's leading companies (CISOs, CSOs, CIOs) that form ASIA's Executive Advisory Board for Cyber (EABC) are not supportive of such a scheme</p>	<p>Two out of three students who do a placement (like work experience or an internship) become full time employees of the host organisation.</p>
<p>Executives said that accreditation was unnecessary, would need to be complex to be inclusive, and acts as potential hurdle to new entrants into the industry</p>	<p>Smaller businesses are often unable to access these placement programs due to lack of knowledge, costs or staff shortages.</p>
<p>Executives said they do not look for certifications when hiring</p>	<p>Gender, age and neurodiversity are challenges in the cyber security sector. Female participation is very low with only 17% of women making up the cyber security workforce</p>
<p>Of those making the hiring decision, 82% are male, 11% are female and the remainder preferred not to say (7%) or were self described (1%)</p>	

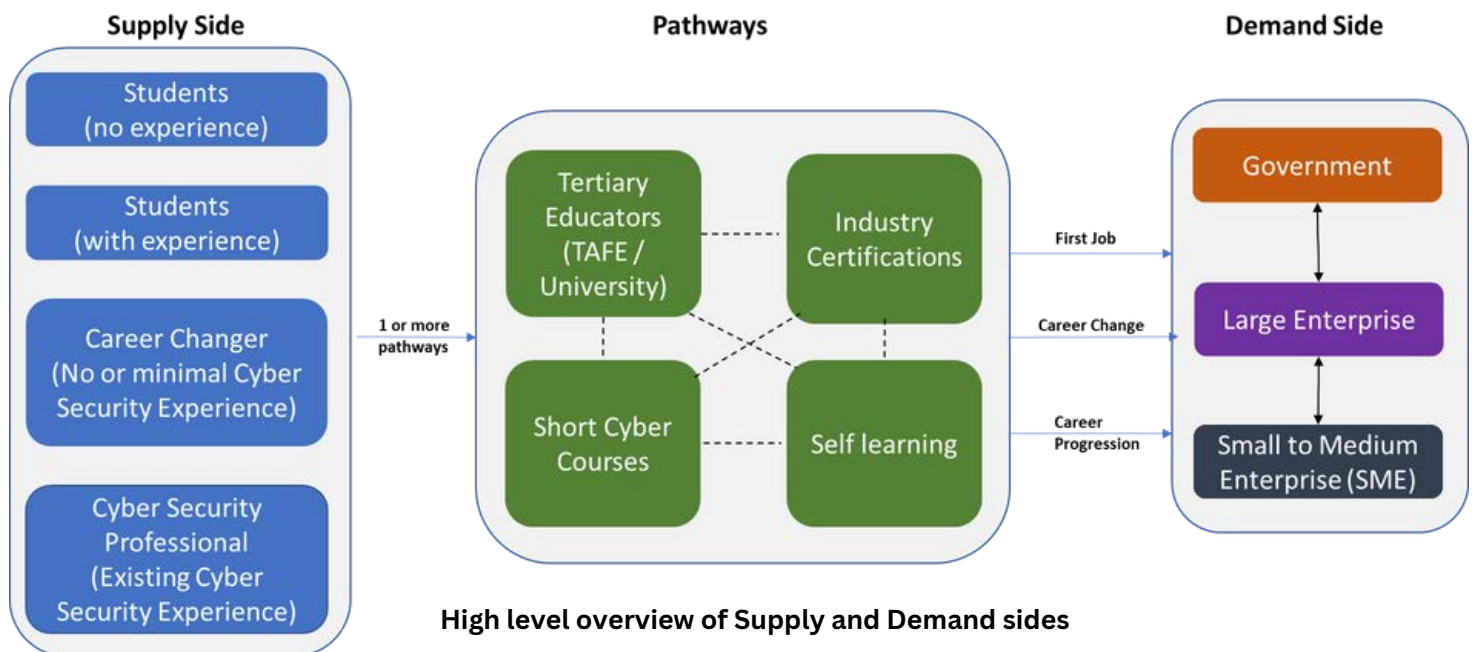
Key Problems in the Australian Cyber Security Sector

	<p>Lack of defined career pathways</p>	<p>Cyber security is a very broad field with many different types of job roles ranging from highly technical through to non-technical roles. Current cyber security courses in Australia do not articulate the pathways into the various cyber security roles.</p>
	<p>Practical pathways for work experience</p>	<p>Needs collaboration between supply and demand side to establish practical pathways for work experience to ensure entrants to the sector via tertiary education complete with hands on experience in industry or government (ie Nursing or Medicine). Outside of tertiary education, practical apprenticeship schemes like trades is missing from the cyber security sector.</p>
	<p>Inconsistent tertiary education</p>	<p>Cyber security courses at university may be developed and owned by a business faculty, IT faculty or shared across both. This directly impacts the quality and type of education graduates obtain in terms of alignment with industry needs. At present there is no way for prospective tertiary students to identify the best course for their career pathway or access comparative rankings of courses from the various providers.</p>
	<p>Certification market saturation</p>	<p>Within the local and international market there are over 460 cyber security related certifications. This complexity creates difficulties and the lack of mapping of the different certifications and pairing them with different job descriptions undermines the value of certifications, making it harder for employers to identify certifications that are relevant to their business needs.</p>
	<p>Varied industry backgrounds</p>	<p>Cyber security professionals enter the workforce from a diverse background. Some have completed tertiary education while others have only completed secondary school. Those who completed tertiary education have entered via Nursing, Law, Education, Humanities, Psychology and a range of other courses as opposed to the traditional IT or cyber security pathway.</p>
	<p>Workforce diversity and inclusivity</p>	<p>Both gender, age and neurodiversity are challenges in the cyber security sector. Female participation is very low with only 17% (an increase of only 3% in 3 years) of women making up the cyber security workforce. In addition, neurodiverse individuals are unlikely to have completed certifications or defined career pathways due to a range of factors, including non-inclusive schooling environments, a lack of supportive and inclusive pathways to higher education (both TAFE and university) and a lack of supportive programs at universities</p>
	<p>Rapid pace of change</p>	<p>The rapid pace of change in the sector makes it difficult for education providers to stay current when some courses are updated every four to five years. The pace of change also exceeds the rate of change for industry in certifications which often set learning objectives for a three year time horizon plus a one year development lag of up to four years.</p>
	<p>Perceived vs Actual Workforce Shortages</p>	<p>Finding qualified and experienced individuals for the workforce has been a challenge in the sector for several years. While the number of cyber security courses generating new graduates has increased, employers are still having difficulties finding suitable candidates and are filling gaps by poaching or recruiting from overseas. It should be noted that not all cyber security graduates obtain employment with many unable to break into the sector when they complete their studies, indicating a wider problem matching supply and demand</p>

Key Findings



Stakeholders on the Supply and Demand Side: Critical for Success.



The supply side of the skills challenge can be summarised as any individual seeking a cyber security career path. Their entry can be through an education provider (TAFE, University or Private), by obtaining any number of global industry certification / accreditations, through networking and obtaining a role based on personality, opportunity (right place right time) and aptitude or by applying through various graduate intake programs if they meet eligibility criteria defined by that host organisation. It is important to note that not all cyber security professionals study a cyber security course, have cyber security related certification / accreditations, but still find a pathway into cyber security via recommendations, introductions, sheer determination, talent or luck.

The demand side is also highly variable with larger enterprises with greater resources running intake programs, working with Universities on what is called Work Integrated Learning (WIL) placements or Industry Based Learning (IBL) placements. Each university has an offering which varies with some placements paid (e.g. student gains an income), some short terms ones that are free (e.g. like work experience) and others which vary greatly in both duration (eg 3, 6 or 12 months) and part-time while studying why others may be a single unit that is completed outside of study, hence classed as a fulltime placement.

No single door exists for industry to leverage the placement programs through university / TAFE meaning it is up to discrete partnerships and an awareness in industry that these programs exist. To add to the challenge, on the supply side a placement often extends a student's course time meaning students are reluctant to take on a placement. However, approximately 2/3rd of those that do, become full time employees of the host organisation. Smaller businesses are often unable to access these placement programs as the students need coaching and mentoring as they learn onsite and these businesses often lack a dedicated IT person let alone a cyber security team.

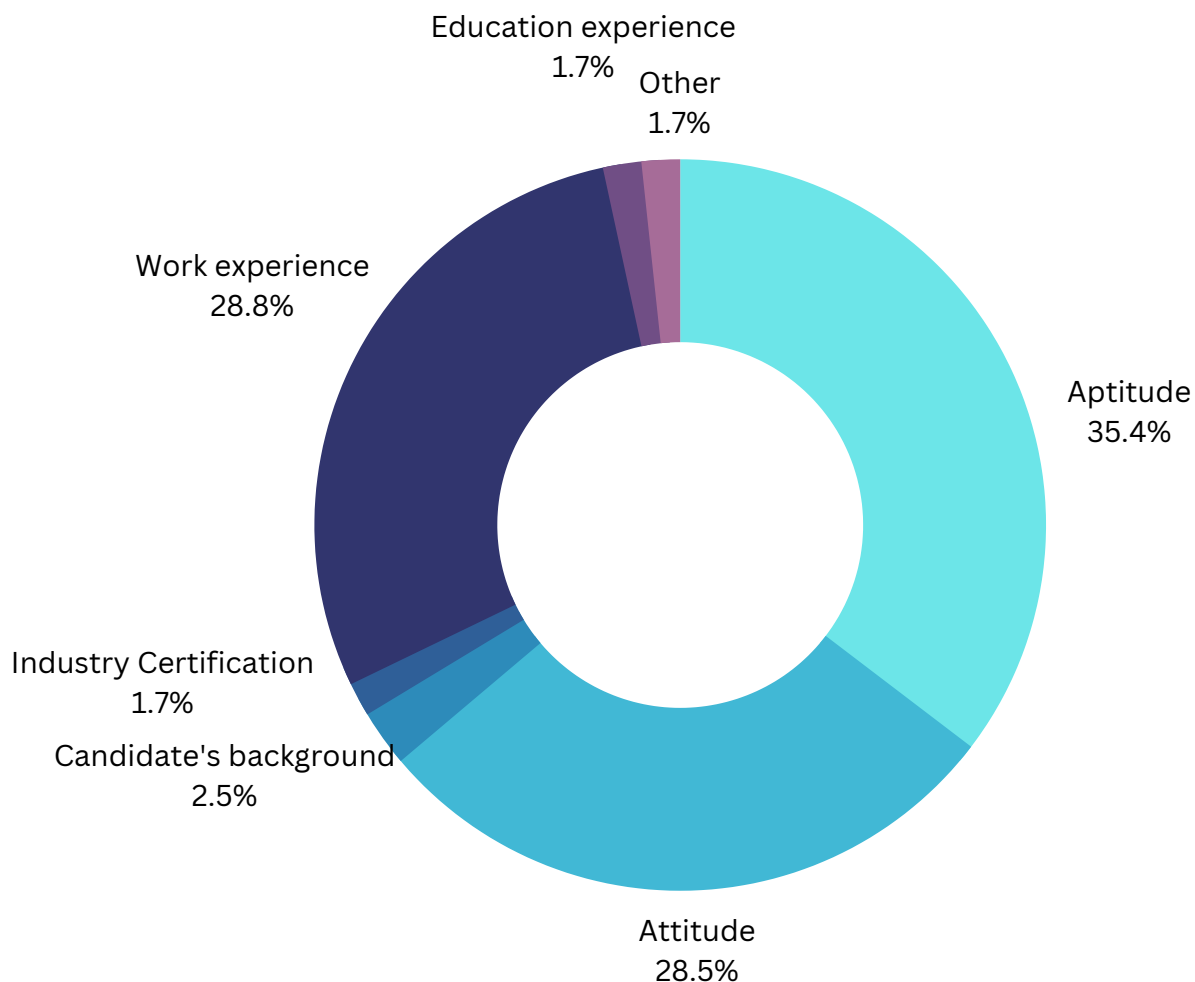
On the demand side, it is easier (but not cheaper) for businesses to poach existing skills out of the market based on an individual's work history and experience in cyber security than to further train graduates or participate in placement programs due primarily to two factors:

1	2
Speed of the individual to become effective in the business is deemed faster by an experienced professional. Graduates can typically take three plus months on average to become effective, while an experienced individual may be deemed effective by the end of their first work week.	Graduates or placements programs required existing staff to coach and mentor the new starters, taking already valuable time out of cyber security teams which are generally under resourced to begin with.

Further challenges on the demand side are compounded when roles are advertised, often attracting hundreds of applicants with no easy or systematic way to determine suitability other than crudely relying on candidates having industry certifications to act as a proxy for competency or knowledge. This crude mechanism means candidates with the right aptitudes, education background (from University / TAFE etc) may be disadvantaged due to a lack of ranking of courses in the sector. While Universities may be ranked based on their research output, it cannot be used as a proxy for the suitability of a course they may offer as cyber security course offered by a business school will vary greatly from an IT school.

When asked to rank the MOST important element, hiring managers overwhelmingly chose three areas in influencing hiring decisions; aptitude, closely followed by work experience and then attitude. The least selected was industry certifications. Some hiring managers commented they use organisational cultural fit and trustworthiness to influence their decision making.

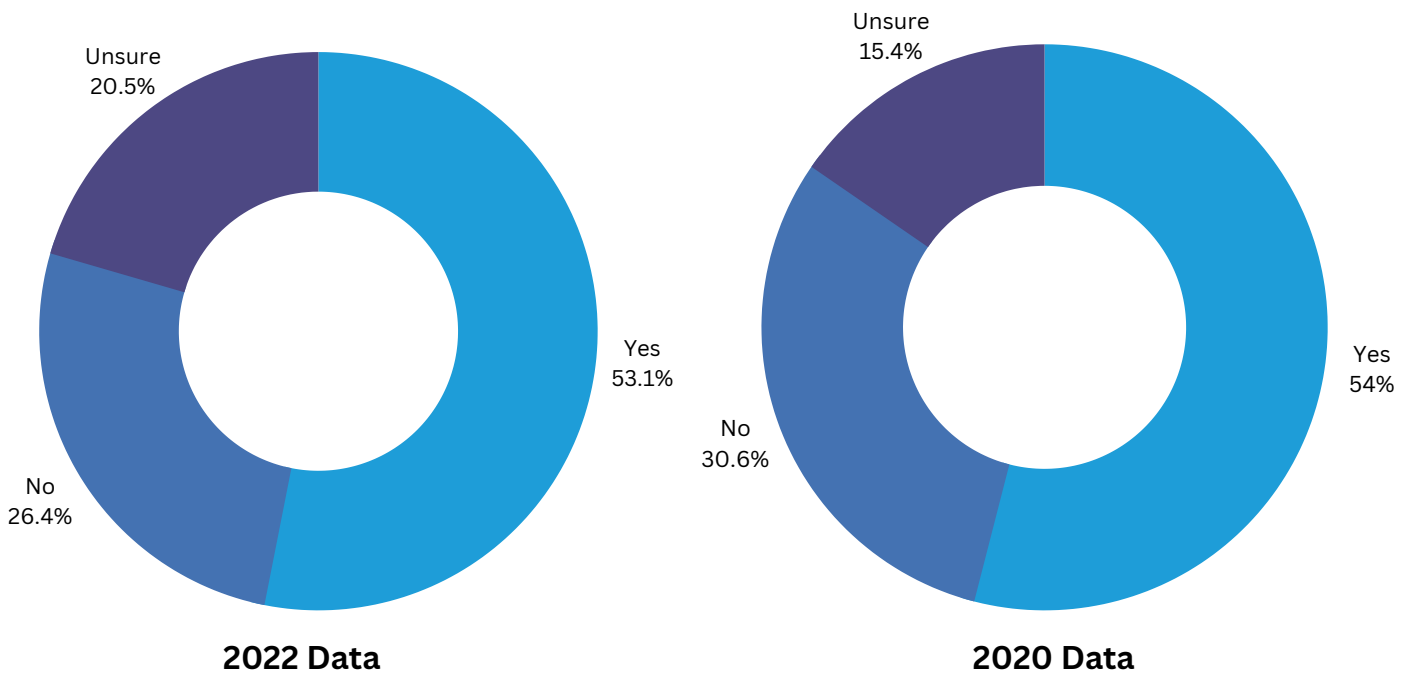
Skills Highly Sought After By Hiring Managers



Support for industry accreditation is mixed

Slightly more than half (53.1%) of AISA's members want to see regulation and accreditation of the sector to ensure a base level of qualification and standard. It is notable that although only about a quarter (26.4%) of respondents do not want a certification scheme and the remainder (20.5%) are 'unsure'.

It is notable that there were very strong feelings expressed by some members in the "No" category that they do not want regulation imposed on the industry. An analysis between 2022 and 2019 indicates support has dropped very slightly with more cyber security professionals unsure. If forced to make a binary decision, a study conducted by AISA in 2019 found almost one in three cyber security professionals do not support accreditation.



Industry leaders not supportive of accreditation

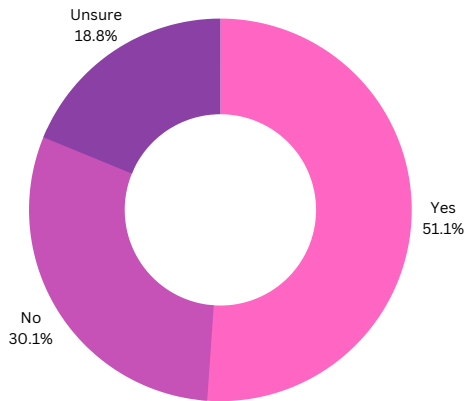
AISA moderates an Executive Advisory Board for Cyber (EABC), comprised of 60+ CISO / CSO / CIOs from across various major industry sectors across Australia. The group's feedback on the concept of accreditation of the cyber sector is that it is unnecessary, complex to be inclusive, and acts as a potential hurdle to new entrants into the cyber security industry. It was also stated that most CISO / CSO / CIOs do not look for certifications when hiring. The EABC are more interested in how the industry could better support:

- pathways into cyber for freshers (new entrants from other sectors) and cyber security graduates
- development for cyber professionals into leadership roles

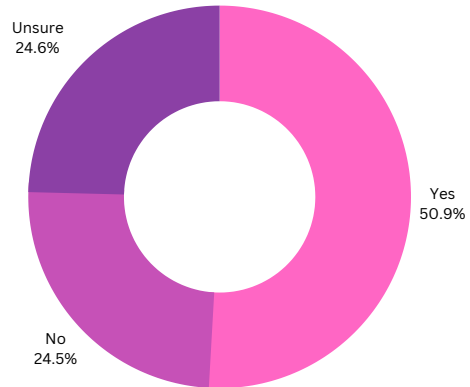
Biggest support for accreditation of the sector appears to be in the education / academic / researcher space (73.8% in favour and 14.8% rejecting the proposition). The lowest level of support for accreditation is within the Executive / C-Suite and leader market segment (43.5% in favour and 40.5% rejecting the proposition) which raises serious concerns as these individuals are key stakeholders on the demand side when it comes to employment and defining the direction of the sector.

Breakdown of accreditation by persona: Do you believe the sector needs accreditation?

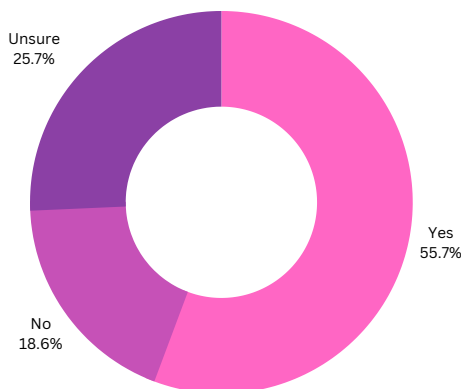
Cyber Security Professional (Technical)



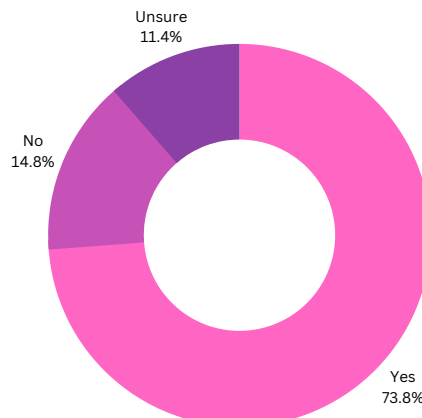
Cyber Security Professional (Non Technical)



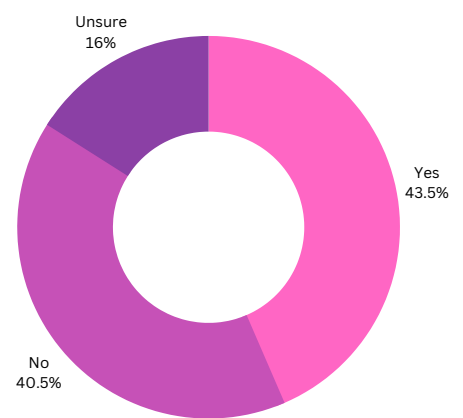
Business Professionals



Educator/Academic/Researcher



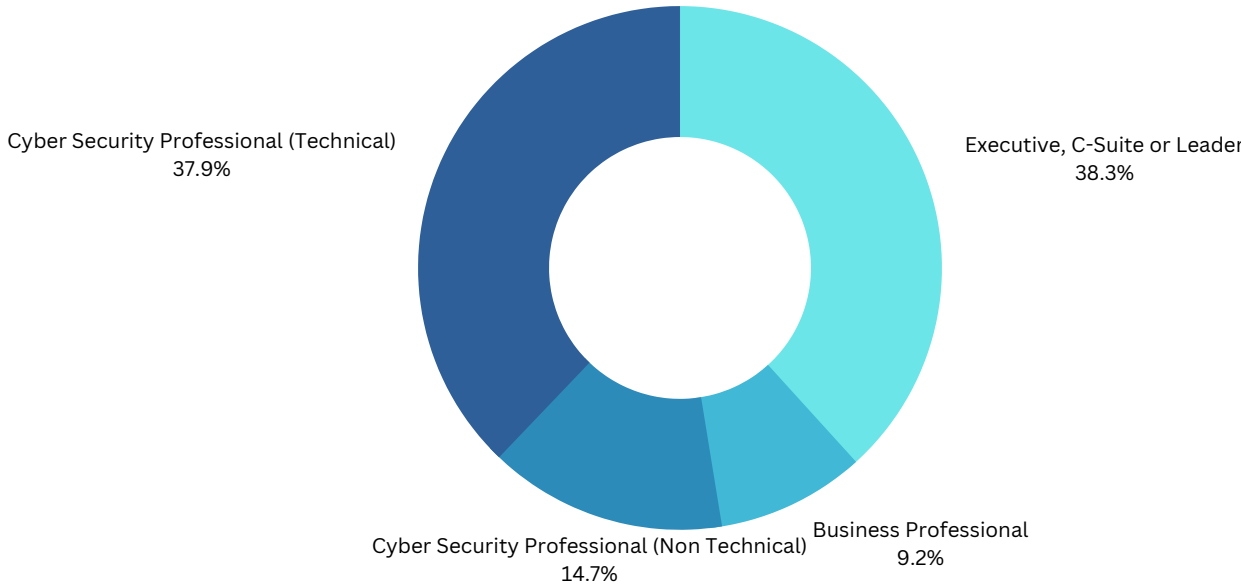
Executive/C-Suite or Leader



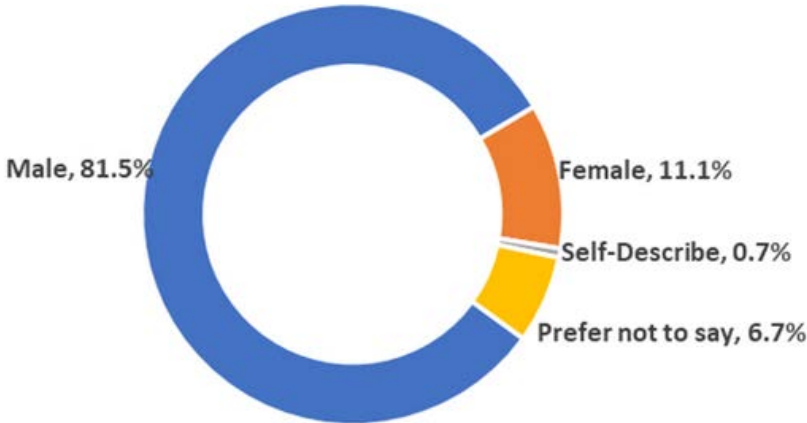
Hiring managers or those actively involved on the demand side can be classified into four broad categories:

- Executives, C-Suite or Leaders
- Business professionals
- Technical cyber security professionals, and
- Non-technical cyber security professionals

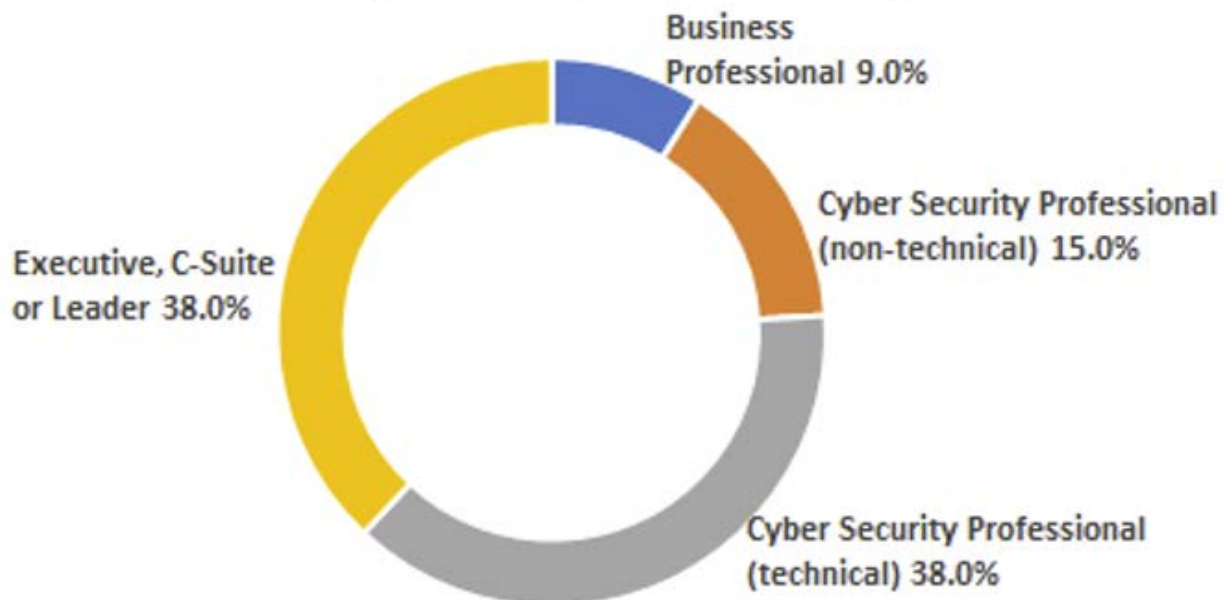
Each class of hiring manager reflects the broad spectrum of cyber security positions within an organisation from leadership through to SOC analysts and GRC specialists. Smaller organisations have less cyber security role types and opt more for cyber security generalists as opposed to specialists.



Gender diversity among hiring managers within the industry The data highlights an imbalance in gender diversity within the decision makers on the demand side (e.g. hiring managers). The industry is still very male dominated with 81.5% of males involved in the hiring decision compared to 11.1% females actively involved in hiring for the cyber security professionals. This skew towards males selecting the future workforce may perpetuate gender diversity issues within the sector.



Gender diversity among hiring managers



Breakdown of hiring managers by role type

An analysis of hiring managers regardless of gender, indicates that almost one third (32%) do not have any industry cyber security certifications while 68% have some type of industry certification. When asked about tertiary education relevant to cyber security, 77% of hiring managers regardless of gender have completed some form of formal education while only 23% have not completed any type of tertiary education.

Hiring managers or those actively involved on the demand side can be classified into four broad categories:

- Executives, C-Suite or Leaders,
- Business professionals,
- Technical cyber security professionals, and
- Non-technical cyber security professionals.

Each class of hiring manager reflects the broad spectrum of cyber security positions within an organisation from leadership through to SOC analysts and GRC specialists. Smaller organisations have less cyber security role types and opt more for cyber security generalists as opposed to specialists.

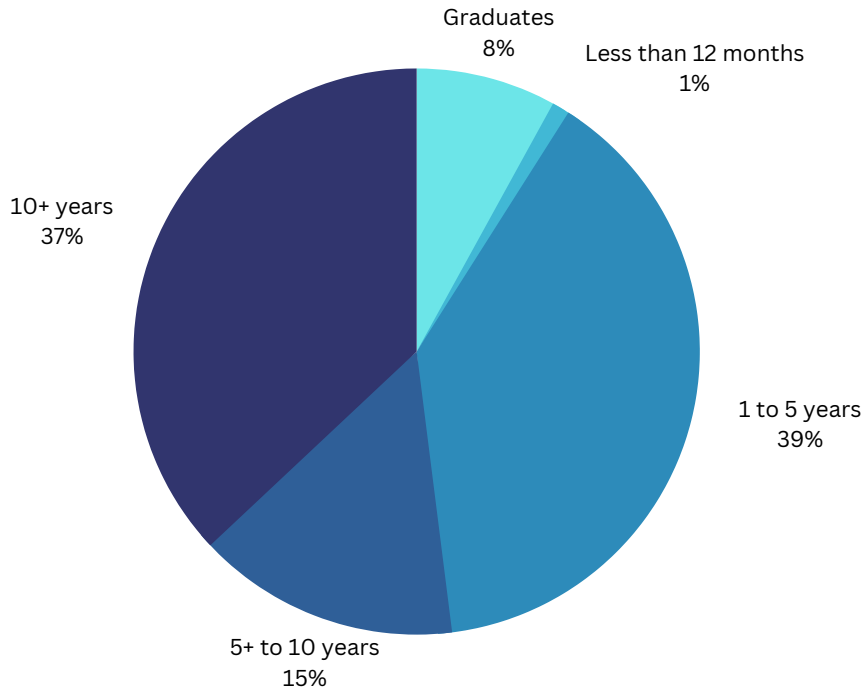
Industry certification is not consistent in the sector and currently disadvantages women.

Not all cyber security professionals currently hold cyber security related certifications and nearly half (**47%**) of all cyber security professionals lack any of the 460 existing available industry certifications. An analysis by gender highlights a concerning aspect where less women in the sector are certified compared to men. For example, **65.7%** of female and **43.4%** of male cyber security professionals lack any industry certifications representing a **22.3%** difference. Compared with tertiary education in a field related to cyber security or with skills transferable to the cyber security sector, the results for male and female respondents only has a 4.2% variance. On average **77%** of cyber security professionals have a tertiary education background in a field relevant to cyber security.

Average years of experience in the cyber security sector is 5.4 Years.

While 37% of people in the sector have over 10 years of work experience, 55% have less than 10 years of work experience and another 8% represented by graduates have little to no practical work experience. Based on one of the key criteria used by hiring managers (e.g. work experience), the 8% represents a large impediment to growing the sector and meeting the needs of the demand side.

Based on research performed by AISA in 2020

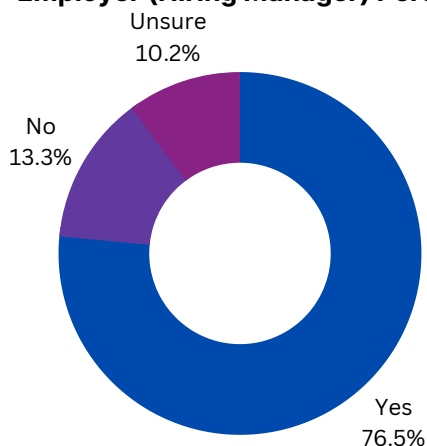


Majority in industry believe there is a skills shortage in the sector.

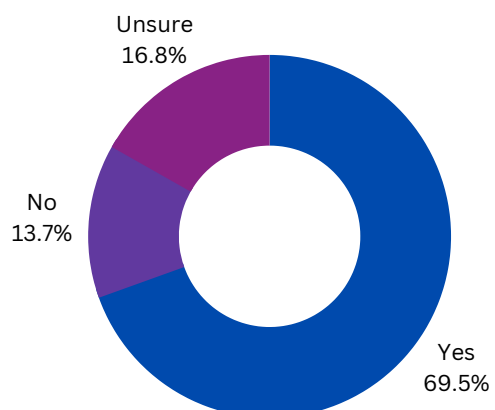
Overall, 72.5% of cyber security professionals believe there is a skills shortage of capable cyber security professionals in Australia. The sentiment of a skills shortage is greater among hiring managers and those actively involved in recruitment (employers) as opposed to those who are not hiring managers (employees). An almost equal portion of both employers and employees feel there is no skills shortage (e.g. 13.3% to 13.7%) with a larger portion of employees unsure if a skills shortage exists.

Is there a skills shortage in the sector?

Employer (Hiring Manager) Perspective



Employee Perspective



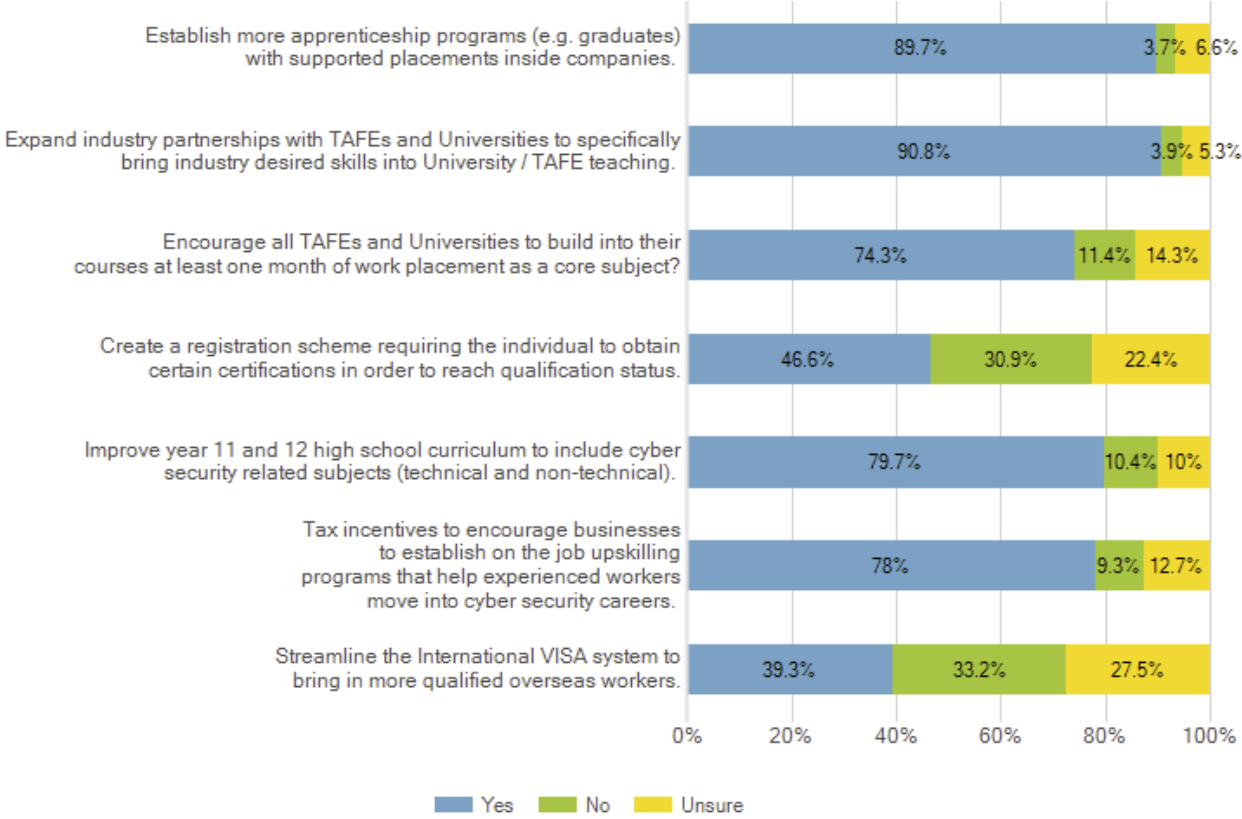
Commentary collected from cyber security professionals also highlights the sentiments that there is a conversion problem, translating new graduates into full time paid employment. This conversion challenge may be related to a lack of hands-on work experience in the tertiary education sector in cyber security courses or it may be related to an inability for employers to gauge the effectiveness of cyber security training programs and allocate appropriate staff to coach and mentor new graduates.

Other factors are likely to impact the conversion such as a graduate's industry social network, their approach to job applications, the structure and focus of their Curriculum Vitae (CV) and importantly their aptitude and attitude if they are lucky enough to get to an interview. With the number of students completing the numerous cyber security courses at University and TAFEs across Australia, the question needs to be asked, where are they finding employment in the sector? There are numerous stories of graduates from a Bachelor or Master level of study finding it very difficult to break into the cyber security sector.

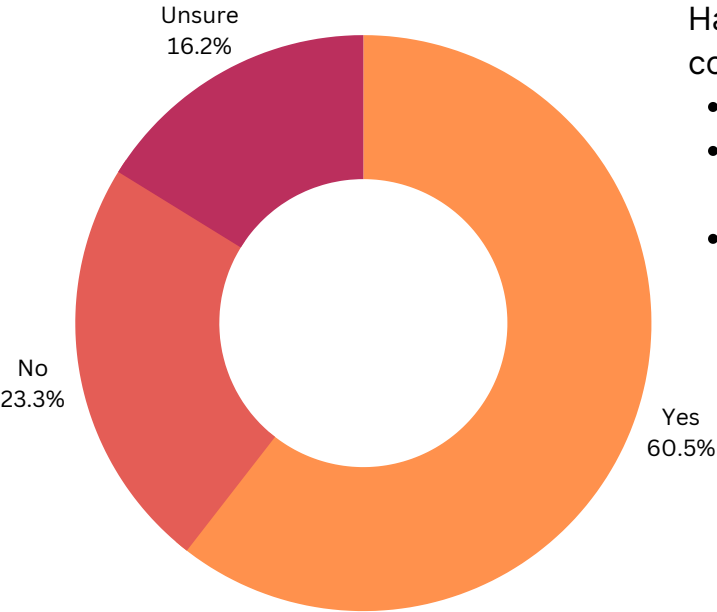
Tertiary education could help to address the workforce shortages by incorporating work experience as part of their core curriculum, similar to other sectors like medicine and nursing. Most respondents felt Australian consumers would benefit if there was a way to rank and compare higher education cyber security courses offered by the various education providers. This would be a good step forward to provide transparency in the market and encourage cyber security courses to improve in a timelier fashion and align with the needs of industry. It also provides consumers with a one stop shop to search for and identify courses that meet their needs (i.e. online, in person, part-time, evenings etc) highlight courses based on career pathways (i.e. leadership, technical, non-technical or generalist) and provide rankings based on specific criteria such as their student employment success rates, placement numbers, course content and alignment to industry requirements.

The other aspect for consideration is employment of staff from non-traditional cyber security sectors. A wealth of talent exists as career changers, individuals who want to cross over into cyber security or new graduates from other course backgrounds such as humanities, sciences, education and law. If the sector is forced to adopt an accreditation or licensing scheme it needs to be inclusive and open to cater for the wealth of talent from non-traditional pathways.

Cyber security professionals were asked to rate options that would help address the skills shortage in the sector. The two least favoured responses related to VISA changes and establishing a registration scheme.



Cyber security professionals were asked if Australian consumers need a way to rank and compare higher education cyber security courses offered by various education providers to help consumers select the most appropriate course for their career needs.

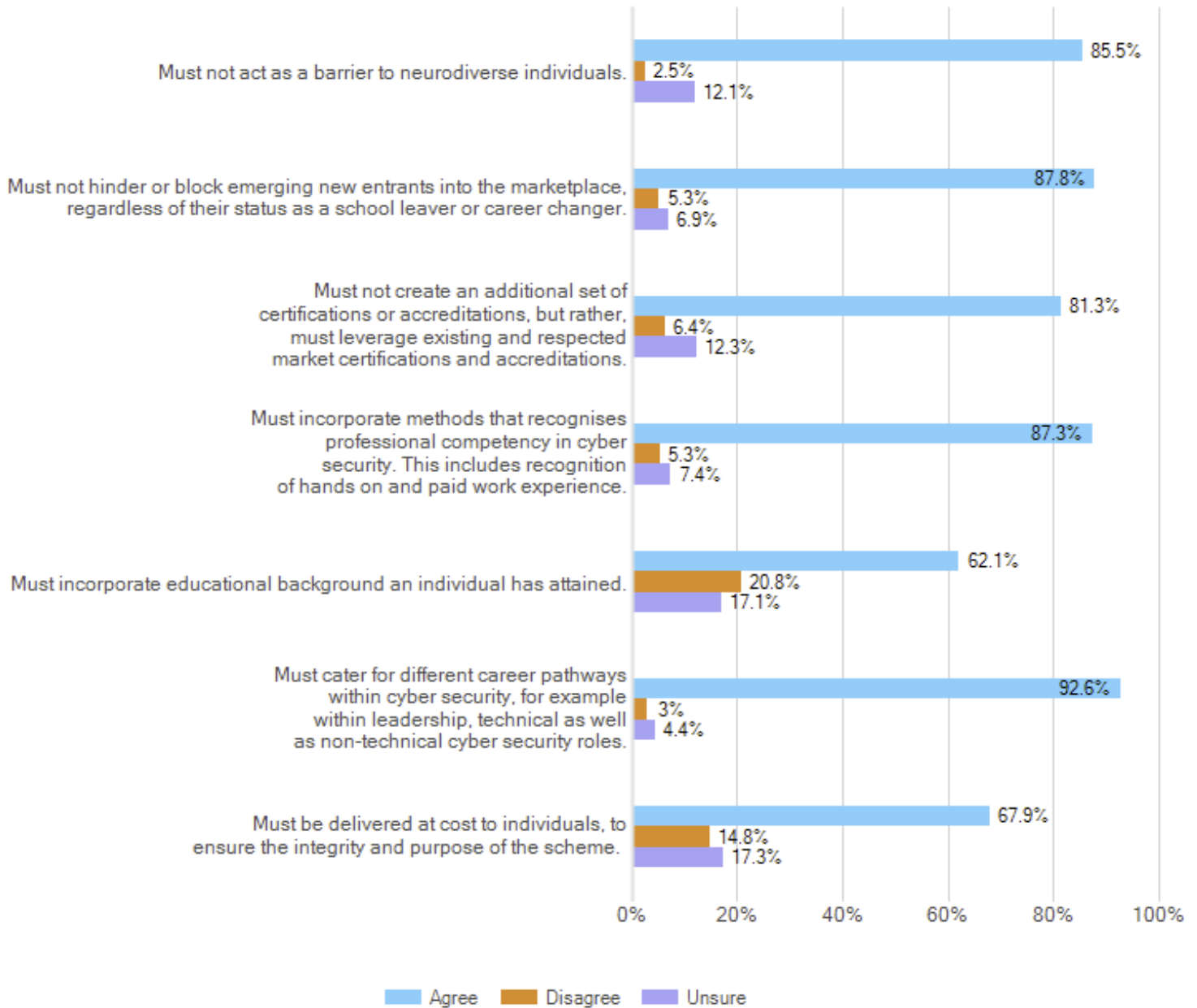


Having a centralised place for consumers to compare cyber security courses would enable:

- greater transparency in the market
- alignment and relevance of courses to the needs of industry
- consumers to search based on various criteria

Principles that should be included in an accreditation scheme

For any accreditation scheme to be successful in a complex sector, it needs to be underpinned by a set of core principles and values. We asked the sector to rate the importance of various elements that may underpin an accreditation scheme.



What accreditation could include

When asked what elements an accreditation scheme should incorporate, the answers were understandably mixed across the sector. The following key themes were present in the answers from respondents:

- Continuing professional development
- Support for early career entrants and different pathways
- A code of conduct or set of ethical guidelines
- A tiered approach that caters for various levels of experience or qualification, including technical, non-technical and leadership
- Accessibility for all individuals
- Contributions back to the community such as volunteering or mentorship
- Character, competency and experience checks

Case Study

"I graduated after completing a Diploma of Cyber Security Studies at a major Australian University. I'm also self-learning AI and Machine Learning to improve my chances of getting a job and I'm a mature age student with extensive background as a telecommunication engineer. So many roles are looking for a minimum of 2 years of specific cyber security experience with additional skills like networking or software development which makes it difficult to apply for job roles. My course only offered limited intern placements and so, many students from my cohort are having difficulties getting jobs."

Australia's first female Prime Minister giving a keynote at Australia's premier cyber security conference in Canberra



About



AISA

The Peak Membership Body for Cyber and Information Security

Australian Information Security Association (AISA)

As a nationally recognised not-for-profit organisation and charity and as the peak membership body for cyber security professionals, the Australian Information Security Association (AISA) champions the development of a robust information security sector by building the capacity of professionals and advancing the cyber security and safety of the Australian public as well as businesses and governments in Australia.

Established in 1999, AISA has become the recognised authority on information security in Australia with a membership of over 9,500 individuals and corporate partners across the country. AISA caters to all domains of the information-security industry with a particular focus on sharing expertise from the field at meetings, webinars, conferences and networking opportunities around Australia.

AISA's vision is for a world where all people, businesses and governments are educated about the risks and dangers of cyber attack and data theft, and to enable them to take all reasonable precautions to protect themselves. AISA was created to provide leadership for the development, promotion and improvement of the information security industry.

AISA's strategic plan calls for continued work in the areas of advocacy, diversity, education and organisational excellence to ensure that all Australians are cyber safe and secure online.



Acknowledgements

AISA acknowledges the significant contribution of the following individuals in this report:

Damien Manuel - Board Chair, AISA
Dr Suelette Dreyfus - Board Director, AISA
Michael Trovato - Board Director, AISA

Akash Mittal – Board Director, AISA
Chloe Hatzis – Company Secretary, AISA



Damien Manuel is an Adjunct Professor at Deakin University's Centre for Cyber Security Research & Innovation (CSRI) and the Chairperson of the Australian Information Security Association (AISA), a not-for profit organisation which aims to improve Cyber Security in Australia at a Government, Industry and Community level. Manuel also provides advice to several boards both in Australia and internationally. He is a well-known leader in the Australian cyber security sector and works closely with both federal and state / territory governments.



Chloe Hatzis is a Data Security Specialist internationally experienced at implementing information security. She has an LLB (Hons) and nearly a decade of experience in business operations, cyber security strategy, international privacy and data protection law, information security management, corporate governance, and cyberlaw training for executive level management.

Chloe currently volunteers as the Company Secretary for the Australian Information Security Association (AISA). She has been active in the AISA community since 2018 and previously held the position of Deputy Branch Chair for the Melbourne Executive Committee. Her unique skill-set enables her to bridge the gap between implementing law, technology, business process and security to empower individuals and organisations to make informed decisions about their information. Chloe received the AISA 'Volunteer of the Year' award in 2018 and was nominated for 'the One to Watch' in the Australian Women in Security awards 2019.



Akash Mittal was appointed as the AISA Board Director in December 2021. He has been an active member of the cyber community for many years. Akash has a number of years of experience working within the industry in Australia and New Zealand. Akash holds a Master of Science degree and several other industry qualifications.



Dr Suelette Dreyfus is a Senior Lecturer in the School of Computing and Information Systems at the University of Melbourne. She leads the core undergraduate subject in digital privacy and security and co-runs Masters-level teaching in Emerging Technologies. She graduated from Columbia University before going on to complete her PhD at Monash University.

Suelette leads research projects in the digital privacy and security space, with a particular focus on consumer protection. She has previously co-designed and run projects in e-health reporting of errors in hospitals and exploring barriers to technology adoption in the health-setting. She has expertise in media and has previously trained at and worked on the staff of one of the largest selling daily newspapers in Australia as a journalist. She introduced the first digital security training for Master's journalism students at her university. She appears regularly in international and Australian media speaking on her areas of expertise.



Mike Trovato joined IIS in 2018 with over 40 years' experience in consulting and financial services in Australia, Asia Pacific, and the USA. He is a cyber security, privacy and technology risk advisor to boards, board risk committees, and executive management.

Mike focuses on assisting key stakeholders with understanding the obligations and outcomes of effective privacy and cyber security. This includes solving an organisation's issues with respect to regulatory, industry, and company policy compliance and to protect what matters most in terms of availability, loss of value, regulatory sanctions, or brand and reputation impacts balanced with investment.

**Please refer to the AISA website for full Board Director profiles:
www.aisa.org.au/Public/AboutAISA/Board_of_Directors.aspx**

We thank you for considering industry feedback



Australian Information Security Association (AISA)

ABN 181 719 35 959
Level 8, 65 York Street
SYDNEY NSW 2000
AUSTRALIA
www.aisa.org.au
info@aisa.org.au

Prepared, authorised and published by the Australian Information Security Association (AISA)
Level 8, 65 York Street, Sydney NSW 2000

© Australian Information Security Association, September 2022