

AustCyber

Part of the Stone & Chalk Group

Quarterly Report

1 January 2023 to 31 March 2023

Australian Cyber Security Growth Network Limited
to
Department of Industry, Science and Resources

Australian Cyber Security Growth Network Ltd
An Australian Government Industry Growth Centre
Unit 2, Level 4, 1 Hobart Place, Canberra City ACT 2601
ABN 73 616 231 451

S22

S22

S22

S22

S22

b. AustCyber run events and workshops

Date	Description	Attendees	Location
07/02/23	Australian Cyber Security Professionalisation Program (ACSP) co-design workshop three - focused on Professional Standards and Frameworks	10 Co-design team members (industry leaders/experts)	Melbourne - KordaMentha office
23/03/23	ACSP co-design workshop four - focused on Professional Recognition Scheme design (part 1)	11 Co-design team members (industry leaders/experts)	Canberra - Australian Computer Society office

c. Skills building activities

Australian Cyber Security Professionalisation Program (ACSP)

During this reporting period:

- Two face-to-face co-design team workshops were delivered focused on:
 - Agreeing on the need and value of professional standards and agree on the skills frameworks to include - 7 Feb 2023
 - Agreeing on the need and value of an accreditation or recognition scheme (part 1) - 23 March 2023
- The qualitative customer research was completed.
- Regular briefings continued with key stakeholders throughout the period.
- In early January the program team began engagement with the UK Cyber Security Council and UK Government.
- The ACSP program was publicly announced via a joint media release with the co-design team partners in late March. Example articles:
 - <https://eglobaltravelmedia.com.au/2023/03/30/austcyber-launches-australian-cyber-pro-program/>
 - <https://www.arnnet.com.au/article/706680/austcyber-organised-group-to-establish-aussie-cyber-security-standard/>
- A high level proposal and budget for phase two of the program was prepared and presented to DISR for consideration in early March.

- Work began drafting an ACSP report detailing the outcomes and outputs achieved from phase one and a high level phase two plan including the investment required. This report will be delivered to federal government partners in the next reporting period.

Workshop three and four overview

The third co-design workshop was held in Melbourne on 7th February 2023. The workshop was kindly hosted at the KordaMentha Melbourne office and focused on the need and value of professional standards for cyber security and which cyber security skills frameworks should be included and why.

Workshop four was held in Canberra on 23rd March 2023 to coincide with AISA Cyber Conference being held in Canberra the same week. This workshop was again kindly hosted at the ACS Canberra hub and focused on agreeing on the need and value of an accreditation or professional recognition scheme.

During this period there were a few changes to the co-design team:

- s22 as the representative for the Tech Council of Australia
- s22 AISA joined the team as part of the AISA's succession plan in preparation for s22 later in the year
- ACSC has joined the co-design team and has been represented by s22

During these two workshops the co-design team:

- reviewed and discussed:
 - the key learnings to date from the employee and employer interviews.
 - the four detailed employee personas developed as a result of the qualitative research. The detailed employer personas and high level career pathways will be developed in the next reporting period.
 - what professional standards are and are not. They discussed the UK Cyber Security Council program pilot which includes professional standards and the value of having professional standards for cyber security in Australia. They also looked at other alternatives that could be considered.

- were provided with a detailed spreadsheet of existing cyber security frameworks to review and consider during workshop three. They were asked to provide their feedback on which frameworks should be included or not included and why out of session. Their feedback was presented and discussed at workshop four in Canberra.
- learnt about the UK Cyber Security Council business model including their fee and governance structure.
- reviewed and critiqued a high level 'strawman' professional recognition body inspired by the UK Cyber Security Council business model.

Program outcomes to date

The co-design team has designed and agreed:

- The draft baseline requirements to be recognised as a cyber security professional that will inform the detailed design in phase two of the professional standards in cyber security.
- There is a need and value in having professional standards for cyber security in Australia.
- On the core cyber security skills frameworks to include and why. These frameworks will be mapped and used for detailed development in phase two.
- On the need for and value of a professional recognition body and scheme for cyber security in Australia.

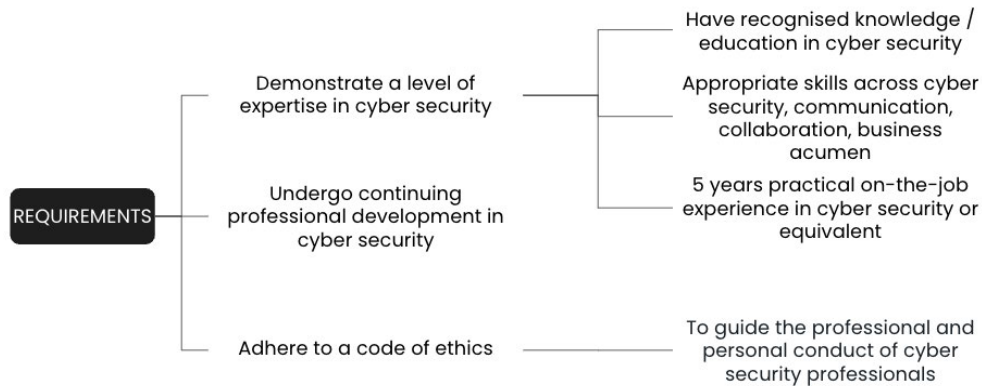
Program outputs to date:

The co-design team has produced:

- A set of requirements, tested with end users, that will inform the detailed development of professional standards for cyber security. These will be developed in phase two of the program.

Agreed baseline requirements

These will inform the professional standards to be recognised as a cyber security professional



- Four detailed cyber security employee personas including: existing worker, new entrant, career changer and international worker. Employer personas and high level career pathways will be produced in the next reporting period.

Existing professional

Recognise where I am already meeting these professional standards/requirements



My title doesn't expressly link to Cyber Security. But I was doing cyber security work before it was (sexy) called cyber security.

About me

I have been working in the cyber security sector for a number of years and more often than not I come from an IT or software engineering background (of which I have worked in for years).

The most significant learning for me has come from working on-the-job.

If I've done certifications I have been selective on which ones as I know which are relevant for my work and career progress, and those that aren't worth the paper they are printed on.

How I define a cyber security professional

A cyber security professional is someone that has a holistic understanding (people, process, technology) of what cyber security is, its risks and impacts to individuals and organisations.

Technology is important for a cyber security professional to understand but the level of technical application is dependent on their role.

MY CHALLENGE		
I am already here I've been in the industry for 20 years, I have the experience, and my peers already recognise me. <i>Now? I don't think I would jump into it. Because I think I've already made my mark in the company that I want to work in. So I'm recognised and I don't think I have a need to prove with an external certificate like that.</i>	The industry is changing and moving fast If I'm not on top of the constant changes in the industry I run the risk of not being up to date for my role.	It's not a one size fits all The industry is maturing, we need to recognise the broader range of skills required to perform the diverse job roles. <i>There's all these niche areas. There's so many different spaces, and they are all very different job roles, and they're speaking to different people.</i>
MY NEEDS		
Recognise where I am already meeting these professional standards. Allow me to include experience I have gained through years working in roles relevant to cyber security.	Reduce the noise. Create a one-stop-shop for information and standards that is governed by an organisation I trust and value.	Understand that rigid pathways don't work in Cyber Security. Acknowledge there are a wide variety of jobs, with many relevant pathways for people to be recognised. <i>The journey is not the same for anyone and I don't think it should be a set journey to be a professional.</i>
WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME		
Professionalisation acknowledges and formalises the ecosystem that is cyber security. If the standards I am already meeting can be used for my recognition. The professional standards need to be more than words on-a-page or boxes to tick. They need to be upheld so that we lift the quality of the sector.	It needs to recognise the non traditional ways I learn about cyber security. Provide clarity on what the quality certifications / qualifications are.	By providing official pathways for my continued growth and development and ensuring that these pathways cater for the diversity we want in the sector. It needs to value on-the-job experience / training as much if not more than education.

Photo by Emmy E. from Pixels

Career Changer

Recognise what I bring to the sector and guide me on where to focus my time and effort



As a career changer, I wouldn't consider myself a professional yet – I need to build up my cyber security specific experience.

Photo by Anna Shvets from Pexels

About me

I have a background (and hold some qualifications) in another industry, so I have the soft skills and a basic knowledge of cyber that allows me to enter the industry. I moved into cyber security because external (and internal) pressures led me to it. I've always been interested in IT and technology and cyber security is a growing industry with many career opportunities.

How I define a cyber security professional

A cyber security professional has been in the industry for a while – they know more. They should be able to identify the risks and protect the company or any organisation. They can identify, protect, and detect. They can respond to the incident and develop something to reduce the impacts of the events, and then finally, they can help the company to recover.

MY CHALLENGE		
I don't have peer recognition I'm new in the industry and need to build credibility amongst my peers. <i>I think just the recognition to be accredited would be enough for me. You know it should be like an industry currency that not just everyone can have access to, so the recognition alone from that would be valuable.</i>	My background isn't in IT You don't need to spend years learning IT technical skills but I think it's important to understand the basics of IT. <i>I know people who've moved into CISC from having a technical background have found it a lot easier. Because they already have that foundational knowledge – especially people who come from IT backgrounds or have worked in other technical roles.</i>	It's hard to keep up It's hard to keep up with the latest skills – once I finish a course or learn a new technique the landscape of the industry has already changed, it's so hard to keep up.
MY NEEDS		
I need some sort of currency within the industry.	I need to understand the key principles that underlie how cyber security works, and how organisations can use those principles.	I need to tailor my training and learning to my area of specialisation while still gaining varied experience.
WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME		
A tiered model approach would provide incentive for someone like me with less experience, I could achieve it in the next couple of years. If I can count what I am already paying for that directly relates to achieving this (I can't sign up to all of them).	Clear guidelines and requirements as to what makes a cyber professional. <i>Be clear on what the requirements are for me if I want to be there, I need to do this, this and this. Just be clear, so I know what I have to do.</i>	There is a pathway that includes hands-on experience and doesn't mandate a university degree. Make the pathways clear and recognise the various entry points and relevance of different skills. <i>I don't think it's purely having technical skills because a lot of people have technical skills, but then they lack a lot of soft skills.</i>

New Entrant

There isn't a clear pathway for me to get in and be successful in the sector. I need direction on what choices to make



Give me clarity on pathways so I can invest my time and money wisely.

Photo by Pavel Danilyuk from Pexels

About me

I have recently entered the industry after moving away from my previous role. I got a certification in IT or Cyber Security to help me break into the industry. I have little to no on-the-job cyber security experience so I have been placed in an entry-level role. The most important thing for me is to get the hands-on experience so I can progress in my career, and be recognised as valuable in my role.

How I define a cyber security professional

A cyber security professional is someone who has had years of experience in the industry, and has the knowledge/theory to back them. They have a foundation in IT and demonstrate 'professional' skills.

MY CHALLENGE		
Entry level jobs require experience How can I gain industry experience, when employers are asking for 1-2 years experience for entry level roles? <i>There's very limited entry level jobs, and if so they want 1-2 years experience.</i>	I don't know what certifications are valuable Am I wasting my time and money on something that won't get me employed? There isn't a clear pathway to help me decide on which one to do. <i>I have studied 16 certifications and maybe two were effective.</i>	The pathways are unclear I struggle to understand and describe what a professional is because there is a lack of clarity on how to get there.
MY NEEDS		
Tell me where the best place to start is and what I need to do to get in there.	Show me what certifications are valuable, so that I spend my time and cash on something that is credible. <i>Companies out there aren't looking at what degree you have studied, they are only looking at certifications, or ask for previous experience (2 years) in similar industry.</i>	Help me understand what a professional is to give me a goal to work towards <i>I don't think I have enough experience to understand what the requirements of a professional should be.</i>
WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME		
Tell me what employers value and where I can look for a job. Pathways that recognise all my relevant hands on experience, not just experience after I've finished my graduate program/role. <i>I would have spent 4 years studying then 5 years in the industry, 9 years is a long time to be recognised. If you do it parallel then it works.</i>	Guidance on potential pathways, and helping me understand how to work my way up in my career. It doesn't require me to pay for another annual fee/ membership.	A tiered approach to professionalisation so I gain recognition at multiple stages of my career. <i>If we do a tiered level of experience: Junior: 1-2 years Mid: 5 years CISO level 10 years.</i>

International worker

Ensure my international certifications and skills are recognised in Australia



To increase migration to Australia, you want to have something that can at least be interoperable with other countries.

About me

I migrated to Sydney last year from <country> for opportunities in cyber security. Before I migrated to Australia, I worked in IT. I was in the cyber security space in <country> for more than five years. I have, at a minimum, a bachelor's degree and multiple certifications, and I often have come in via the Global Talent Program visa.

How I define a cyber security professional

For someone to be considered a professional, they need proven work experience. When I worked in <country>, there were guidelines from a governing body of what a cyber professional is, including a reference framework to show the level of experience a professional has and their progress. It also has interoperability with certifications in other parts of the world.

MY CHALLENGE

Having to do things twice

I've done that [background check] as part of my visa entrance process, so I should not have to do it again.

If it means I have to do extra, extra training, or I have to undergo exams in order to do this, then I'd have to weigh up the value. I probably wouldn't do it.

There is no interoperability with Australia

ISACA, (ISC)2 etc, are recognised internationally but have yet to be applied under a nationally consistent approach in Australia.

If we put a national requirement, it shouldn't be limited only to Australian nationals, I think you need to consider the international workforce and how they may contribute to the Australian sector.

MY NEEDS

Recognise where I've met requirements with my (international) experience.

To make the transition seamless, is there a way where we recognise that your clearance, integrity, qualification, and certifications in your home country... when you come to Australia, you don't necessarily have to start again. You can say, well actually, I've already met all of them. So, therefore, I can then be recognised.

Global recognition.

I guess that is a great way to attract the interoperability of the professional - from both sides.

WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME

A framework that substantiates my integrity as a cyber security professional (when I've already been subject to a police or background check).

Plug into what I already have.

If there was a way to plug in recognised certifications and the work you have to do to get them. Therefore if you could plug what you are already doing there and it is acknowledged by the Australian accreditation program that would make the process easier.

Photo by Kindel Media from Pexels

- The high level design 'strawman' of the structure for the governing professional recognition body. The high level business model including membership models and fee structures of the body and scheme will be explored further in the next reporting period.

Strawman: The professional recognition body



Qualitative employee and employer research

The qualitative research was completed during this reporting period. It involved 1:1 one-hour interviews with 25 employees and 20 employers.

Employees interviewed:

- Career changers — previously working in a different industry now in cyber security.
- Existing professionals — working in a cyber security role for the past five years or more.
- New entrants — working in a cyber security role for less than one year after graduating (mix of school leavers and university graduates).
- International workers — moved to Australia within the last five years and are working in a cyber security role. They were already working in cyber security in their home country.

Employers interviewed:

- Non-technology focused small to medium enterprises (SMEs)
- Technology focused SMEs
- Corporates

Research key findings:

- Both employers and employees place a **high degree of value on experience** working in the industry.
- Therefore, when they think of someone operating at the next level, a professional, they want to see a **professional standard that includes relevant experience** working in cyber security.
- Employees are **drowning in the choice** of how they learn about cyber security; this was explicitly called out when talking about certifications.
- Those in the know, people who have been working in the industry for a while, have pieced together their own version of **criteria regarding what certifications they recommend** to their teams or look for when hiring people.
- Feedback suggested that there is **no shortage of certifications, and degrees, that aren't worth the paper they are printed on**, either because they can be

gamed by buying 'brain dumps' online or don't teach you what you need to know to work.

- They see **value in a single source of truth on what is valid** and **having these validated ones being called out in a pathway** to becoming a professional.
- Across the employees and employers interviewed, there was a strong theme for the **creation of a new body to administer professional standards.**
- A **government-backed, industry-supported body was preferred.** Employees expressed that this felt like the right balance as **government backing provided validity**, but not being government-run mitigated the risk of red tape, slowness, and bureaucracy.
- When asked which government department made sense, the **ACSC was referred to as the most relevant** due to its focus, and many employees read and listen to the content they put out around cyber security.
- **Industry-led was called out as the speed and voice** needed to ensure the administration kept up to date.
- Employees suggested that having a **diverse group of industry representatives as part of this body** would bring the balance needed to ensure the continued growth of the industry.
- When employers were interviewed, including AIIA and Tech Council members, they understood **this was not about licensing** but about recognition as a professional; they saw the value for themselves and the industry and were supportive.
- **Recruitment** was a key theme: making hiring easier and having better trust in who is being hired and their capabilities.
- However, if there is a professional recognition scheme, it needs to be **flexible and inclusive, not create a barrier to entry.** It must showcase what each individual brings and not lock people into a traditional model where the only pathway is via formal education.
- It is down to the **individual to demonstrate professional qualities.**

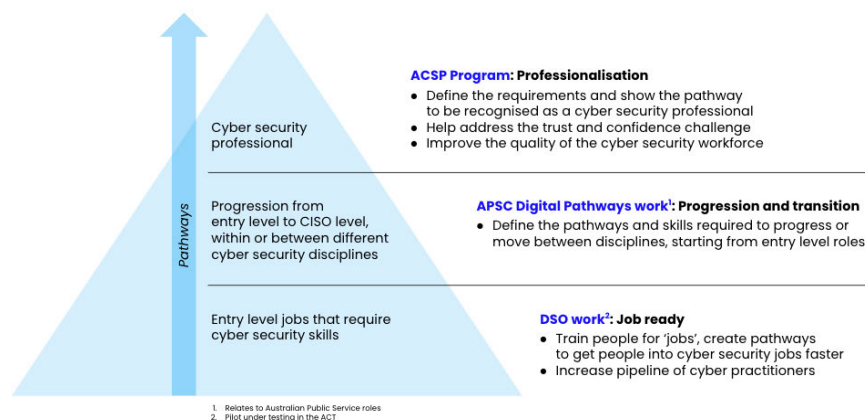
- **People outside the cyber security industry would benefit from having some form of professionalisation** to help them know who they are hiring or what to look for.

Stakeholder engagement

As part of the broader industry stakeholder engagement, the program team is continuing to meet, share, learn from and collaborate with the leads of other related projects and programs. Through these opportunities the team continues to:

- work with the Digital Skills Organisation and APSC and have created a visualisation to represent our respective programs align and complement each other.

Connected programs in cyber security



- engage with the UK Cyber Security Council and UK Government to learn about the UK chartership program currently in pilot. This engagement has provided insight and learnings on the development of the UK Cyber Security Council including their governance and membership structure.

The following meetings and briefings occurred with program stakeholders:

- Co-design team
 - Adhoc individual briefings with team members before and/or after workshops to provide updates on research findings and capture input and feedback on program decisions and outcomes

- Australian Computer Society (ACS), 24 February & 28 March – share with the broader ACS team as well as discuss professional standards schemes in Australia
- Tech Council of Australia, 1 February & 3 March – discuss a succession plan with the outgoing representative (s22) and provide detailed briefing to the new representative Scarlett McDermott
- (ISC)2, 13, 17 & 22 February – introductions and overview discussions, including how to work more closely together particularly during the next phase of detailed design and development
- ISACA, 15 March – introductions and overview discussion, including how to work more closely together particularly during the next phase of detailed design and development
- Government briefings and engagement
 - ACSC, 1 February – update to brief new ACSC team members
 - DISR, 3 February – update and preparations for phase two discussions
 - DISR, Home Affairs, DEWR and ACSC, 16 February – third workshop debrief and feedback/input on decisions and outcomes
 - APSC, 9 March – sharing customer research learnings and respective project updates
 - ACSC, 22 March – briefing for ACSC team members to join the co-design team workshop three
 - DISR & ACSC, 31 March – phase two plan and funding requirements discussion
- Industry stakeholders
 - Engineers Australia, 20 January, 17 February, 17 March – ongoing engagement to share and collaborate on respective programs of work to ensure consistency where relevant
 - Investment NSW, 30 January & 14 March – introductions, overview and Q&A session about ACSP program
 - DSO, 22 February – briefing and update on customer research and outcomes of workshop three
 - UK Cyber Security Council & UK Government, 31 January – introductions and sharing updates and learnings from respective programs

- UK Government, 17 February – sharing learnings and process of the establishment of the UK Cyber Security Council
- Victoria Government Cyber branch, 16 March – introductions, overview and Q&A session about the ACSP program

AUCyberExplorer

During the reporting period, [AUCyberExplorer](#)'s data has been refreshed with new data for the 12 month period 1st February 2022 to 31st January 2023. The most recent data indicates a dedicated workforce size of 51,309 workers with 7,070 jobs being advertised. There are an additional 74,482 workers and 6,090 jobs which are classed as related, meaning the roles are not wholly dedicated to cyber security but require cyber security skills.

s22

S22

S22

s22				
-----	--	--	--	--

Australian Cyber Security Professionalisation (ACSP) program

Current status overview	Please refer to the detailed ACSP program update under c. Skills building activities above Estimated 75% complete
Key activities completed in period (max 5)	Delivered co-design team workshop 3 focused on professional standards and skills frameworks and workshop 4 focused on professional recognition body and scheme

	• Completed customer research and produced four detailed cyber security employee personas • Developed high level 'Strawman' of professional recognition body • Created draft phase one report including high level phase two project plan and investment required for government stakeholders • Publicly promoted the program via joint media release with all co-design partners to start raising awareness of the scheme more broadly
--	---

s22

S22

S22

S22

S22

S22

S22

S22

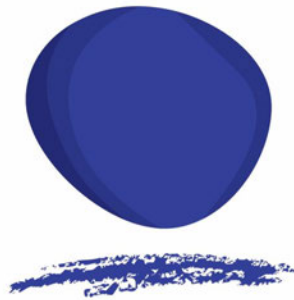
S22

S22

S22

S22

S22



AustCyber

Part of the Stone & Chalk Group

Quarterly Report

1 April 2023 to 30 June 2023

Australian Cyber Security Growth Network Limited
to
Department of Industry, Science and Resources

Australian Cyber Security Growth Network Ltd
An Australian Government Industry Growth Centre
Unit 2, Level 4, 1 Hobart Place, Canberra City ACT 2601
ABN 73 616 231 451

S22

S22

s22

b. AustCyber run events and workshops

Date	Description	Attendees	Location
18 April 2023	Australian Cyber Security Professionalisation Program co-design workshop 5 -focused on Professional Recognition Scheme design (part 2)	8 co-design team members (industry leaders/experts)	Melbourne - RMIT
s22			

s22			

c. Skills building activities

Australian Cyber Security Professionalisation Program (ACSP)

During this reporting period:

- The last face-to-face co-design team workshop for phase one was delivered in April in Melbourne. It was focused on agreeing on the need and value of an accreditation or recognition scheme (part 2)
- Ongoing briefings were held seeking input and feedback with key stakeholders
- Introductions and briefings with new stakeholders to learn, share and identify opportunities for collaboration and input in the next phase including:
 - Professional Standards Councils
 - Hudson, Technology & Projects
 - AWSN – Australian Women in Security Network
 - Tasmania Government
 - Lumify Group
 - Fifth Domain
 - Wise Law
 - University sector – Macquarie University, Melbourne University, University of Tasmania, Deakin, RMIT and Australian Technology Network
- Continuing regular discussions with DISR, ACSC, Home Affairs and the Cyber Security Strategy team to secure and finalise the funding for phase 2.
- The draft Phase 1 report, including the proposal for phase 2 was completed and provided to Government partners in mid April for review. The next version of the report was being prepared in late June to reflect all outputs and outcomes of phase 1 and feedback from Government partners. The next version of the draft report will be provided to Government partners in the next reporting period for further review and feedback.

- AustCyber participated in the Australian Computer Society (ACS) event *Building Tasmania's Cyber Security Professionalism* held in Hobart on Thursday 26th of May.
- Following the public announcement in late March a dedicated [ACSP program website page](#) was created on the AustCyber website.
- Development began on an ACSP marketing plan to raise awareness of the program details, co-design team, stakeholders and plans for the next phase.
- New strategic co-design team members and key stakeholders have been identified and secured for the next phase of the program. *Engineers Australia* and the *Insurance Council of Australia* have agreed to join the co-design team and the Australian Women in Security Network (AWSN) have agreed to be a key stakeholder, particularly in relation to the pilot phase of the program.
- Both the Tech Council of Australia and the Australian Information Security Association (AISA) have formally advised the program team of their decision to step down as an active member of the ACSP co-design team for Phase 2 of the program. Both organisations will continue to be engaged as a stakeholder.
- Work began in May/June drafting high level cyber security specialisms/disciplines relevant to the Australian market that will be key to the next phase of the program. The draft specialisms have been critiqued by the co-design team and will undergo further customer testing and detailed development in phase two.

Workshop five overview

The fifth co-design workshop was held in Melbourne on 17th April 2023. The workshop was kindly hosted at the RMIT University in Melbourne City Campus and focused on agreeing on the need and value of an accreditation or professional recognition scheme – part two.

During workshop the co-design team:

- reviewed and discussed:
 - the three detailed employer personas developed as a result of the qualitative research.
 - outputs and outcomes from the previous session including:
 - skills frameworks
 - the professional recognition body 'strawman'
 - design principles for the scheme
 - high level career pathway

- Completed a financial modelling activity to generate ideas focused on how the professional recognition body will create value in the sector. This activity generated a number of ideas for the ongoing value and sustainability of the body that will be developed in detail and tested in the next phase.

Program outcomes and outputs for this reporting period

The co-design team has:

- critiqued the professional recognition governing body high level 'strawman' and explored financial models for further development in phase two
- produced three detailed cyber security employer personas including: Non-technical SMEs, Technical SMEs and Corporates.

Non-technical SMEs

I've just taken the IT "guy" on through word-of-mouth



Ultimately we rely on third-party SaaS products and our IT company/'guy' for advice

About me

As a small business owner with up to 10-20 employees, cyber security is not a priority for my non-technology-focused business.

We mainly use third-party SaaS products to hold customer data and don't have much data at risk. So while I'm concerned about hacking, system corruption, and scams, we can manage these risks without hiring a dedicated cyber security person.

We rely on our IT company, who I found via word of mouth, for advice. In addition, we have a cyber security insurance to cover any potential risks.

MY CHALLENGE		
I don't understand IT so I put my trust in my IT company/'guy' We hired our IT company/'guy' through word-of-mouth – he was recommended by another small business owner. And he seemed to know what he was doing. The less you know about the topic, the more the recommendations mean.	Finding and selecting the right professional for my needs It's hard to know what to look for when selecting an IT and cyber security professional. I'm not clear on the specific skills and qualifications required.	It's hard to keep up when it's not my focus It's hard to stay on top of the constantly evolving requirements for IT and now with the addition of cyber security, especially when I am a small organisation with limited resources. I think with IT in smaller businesses, there's a lot of trust you're putting in that individual because you're time poor. And it's not an area necessarily of interest for me personally. I didn't set up a business to focus on IT. But it is part of the business.
MY NEEDS		
To trust the IT professional I have hired to perform the required tasks based on objective criteria so that I am not reliant only on word-of-mouth recommendations. I'm not even sure what to look for in an IT professional – it's usually from a word-of-mouth recommendation. There is nowhere to validate that what has been done is correct – except potentially word of mouth case studies.	Guidance on what to look for in an IT and cyber security professional for my specific needs – the qualifications and credentials I should be looking for. Knowing where to look for trustworthy IT professionals in a specific field such as cybersecurity.	Identifying areas to prioritise for my IT, and cyber security, and how to stay up to date with changes in the industry.
WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME		
Having a reliable and objective method for evaluating the quality of work done by the IT professional, particularly for when companies have no expertise in the area. Assurance that the IT professional is current and complies with protocols and processes applied to my IT – particularly for my insurance.	Access to a diverse range of resources and networks, with more experience and knowledge, for seeking advice and recommendations on hiring IT/cyber security professionals, in addition to word-of-mouth referrals.	Easy access to up-to-date and trusted information and guidance on the constantly evolving requirements for cyber security for SMEs. Knowing what areas of my business require cyber security and what I need to do about it. ... the accounts person had a spreadsheet of every single password of the organisation. And then you start thinking about what who has access to that? I'm not sure if that's what you consider cyber security or not.

Photo by Kaitui Subiyanto from Pexels

Tech SMEs

Make it easy for me to hire



I want the hiring process to be easier for myself and for other industries to hire the right cyber security people

Photo by Anna Nakrashevich from Pexels

About me

I own/work for a cyber security startup, and lead a small team.

My hiring practices come from industry connections and recommended applicants with a strong skill set and who are eager to learn.

There's a skill shortage so I need to make sure the people I hire are able to do what I need them for.

MY CHALLENGE

There is a skills shortage

There is a skills shortage in the industry, which has made the hiring process harder. We rely on recommendations and/or we identify qualities and traits that are suitable to bring this person on and skill them up.

Our hiring practices have commonly been through trusted relationships, you come recommended. It's necessary for a small business, they are critical to your businesses success.

There is a lack of clarity on what each role entails

This makes it difficult to determine levels of expertise, recognise previous education and experience, and validate skill sets.

MY NEEDS

If candidates have experience in another area, understand the relevant cross-functional skills and depth of knowledge to make hiring easier.

Employers don't necessarily understand cyber, so it's harder to validate if the employee will be of benefit. They don't know how to validate that person and their skills because of it.

Easily recognisable roles and skill sets across the industry.

Different organisations require different roles/skill sets. In order to make it easier on employers, roles/skill sets need to be easily recognisable across industry - the job description needs to outline exactly what the business is looking for, so if its risk management then it needs to be in the title.

Guidance on which certifications and courses are most valuable and applicable to specific roles, perhaps through the development of a career path framework or hiring matrix.

WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME

Validating and accrediting someone's base level skills in the industry if they have experience in another discipline.

Clear and flexible pathways that recognise education and experience levels.

What you want to build into this model is flexibility and the pathways people can take to get to that professional level.

Provide support for employers to help them understand cyber security and validate employee's skills.

Educate employers outside of the industry on cybersecurity roles and the required skill sets to ensure that they hire the right cybersecurity professionals.

Corporate employers

I find hiring really tricky



Cyber security is an exercise in risk management

Photo by Antonio Sherabao from Pexels

About me

I am working in a senior role overseeing the cyber security for the entire organisation. This involves international teams as well.

My role requires me to think strategically about the cyber security of the organisation and how to engage effectively with my peers in senior management.

I have a number of employees working for me all who have accountability to keep the organisation cyber secure. They have a mixture of technical and non-technical backgrounds.

MY CHALLENGE

Hiring the right candidate is a challenge

It can be hard to find suitable candidates with the necessary skills and cultural fit. It is difficult to accurately identify the skills required for a role and determine a candidate's experience based on their qualifications alone.

The prime candidates do look different across the spectrum of disciplines

There is no clear and framework for defining consistent standards, qualifications and pathways

One that is inclusive of diverse backgrounds and experiences and provides confidence and structure to employers and employees alike.

The risk is that its a free for all out there, and if we are wanting people to come into the industry and have more diversity in the industry its important to give people structure and an idea of how people can ramp up their skillset.

There isn't currently a body that I see as effective, trustworthy, and credible

A model that builds and establishes trust with the right organisational structure.

MY NEEDS

Consistency regarding the level and types of (technical) skills required for different roles and disciplines and how to assess candidates accordingly.

Up-to-date and practical cybersecurity education that reflects the fast-changing industry.

The ability to attract and retain diverse talent in the industry, by recognising and valuing diversity and non-traditional pathways to success.

The creation of a recognised body that is valuable to cyber security professionals and employers.

WHAT WOULD MAKE PROFESSIONALISATION DESIRABLE TO ME

Standardisation of cyber security titles and clarity in the job titles to accurately identify and fill roles. Especially in a constantly evolving industry where new roles are constantly emerging.

Ongoing assessment and development of training programs to keep up with the constantly evolving industry.

A trusted body to provide a framework and pathways to success for individuals, based on experience, skills, and qualifications where relevant from all backgrounds.

To address shortages and prevent salary increases caused by competition for candidates, an inclusive framework that enables more people to enter the industry.

- produced a high level career pathway to be developed in detail in phase two

Pathway to professional recognition



Grandfathering



Recognition



Direction



Interoperability

Obtain recognised knowledge / education in cyber security

- Formal education such as University degree, Masters, TAFE program
- Informal education such as self-learning and micro-credentials
- Appropriate cyber security certifications of authorised members of the professional recognition scheme
- Appropriate cyber security certifications of non-member organisations

Develop appropriate skills in cyber security, communication, collaboration, business acumen

- On-the-job experience
- Appropriate cyber security certifications of authorised members of the professional recognition scheme
- Appropriate cyber security certifications of non-member organisations
- Cyber security traineeship programs

Apply for professional recognition

- Tiered recognition
- Application and assessment through authorised members of the professional recognition scheme body
- Adhere to the code of ethics of the authorised member

Undergo continuing professional development

- Proactive maintenance of appropriate certifications
- Other learning reflective of how cyber security professionals stay up-to-date

- produced design principles to inform the detailed design and development of the scheme in phase two

Design principles

Customer-centered

Designed with the needs and perspectives of mid / experienced practitioners, employers, government, industry, academia in mind. This includes consideration for their diverse backgrounds, experience levels, and career goals.

Continuously improving

The scheme should be regularly reviewed and updated (based on clear measures of success) to ensure it remains relevant, effective, and responsive to changes in the cyber security context. Key stakeholders should have input and influence.

Simple

The scheme should be straightforward to understand and should simplify stakeholders understanding of why you want to become a professional.

Objective

The professional recognition process should be unbiased and objective (vendor agnostic), using valid and reliable assessment methods that are measurable and tangible. It should recognise different types of professionals.

Flexible

Allow for different pathways and entry points to professionalisation by recognising a range of qualifications and experiences, not create barriers to entry, be relevant to current and emerging cyber security threats and technologies, and the needs of the workforce.

Transparent

The professional standards, and the process for professional recognition should be clearly communicated and easily understood by all stakeholders.

Collaborative

The co-design team should engage with stakeholders from industry, government, academia, and the wider community to ensure an appropriate and inclusive design process. Aligned to international partners schemes.

Tasmania event overview

AustCyber participated in the Australian Computer Society (ACS) event *Building Tasmania's Cyber Security Professionalism* held in Hobart on Thursday 26th of May.

This event, supported by the Tasmanian Government, attracted over 50 leaders in Tasmania across cyber security, banking, TAFE, and higher education (Uni TAS). AustCyber's role was to provide a keynote speech from s22 AustCyber to provide an overview of the ACSP Program, participation in the ACSP co-design team panel s22 , and facilitate a workshop over lunch.

The workshop focused on participants generating ideas on how they might contribute to the success of a Tasmanian pilot of the ACSP program. This workshop generated over 50 ideas as well as strong engagement and buy-in to both the ACSP program and AustCyber's role as the nodal player bringing the sector together to solve national challenges. We will continue this collaboration and welcome further ideas and suggestions to make the pilot of the ACSP program in Tasmanian an overwhelming success.

Stakeholder engagement

The following meetings and briefings occurred with program stakeholders:

- Co-design team
 - Adhoc individual briefings with team members before and/or after workshops to provide updates and capture input and feedback on program decisions and outcomes
 - Australian Computer Society (ACS), 21 April & 4 May - program sharing session for input/feedback with Professional Standards Board and Authority, ACS VPs and Chair ACS Cyber Security Committee
 - Australian Information Industry Association (AIIA), 2 May - program briefing and consultation session with AIIA members
 - Tech Council of Australia, 16 May - discuss Tech Council's involvement in the next phase of the program
- Government briefings and engagement
 - DISR and ACSC, 12 April - program update and phase 2 proposal discussion
 - DISR, Home Affairs, DEWR and ACSC, 20th April - fourth and fifth workshop debrief and feedback/input on decisions and outcomes

- Investment NSW, 2 May & 7 June – sharing sessions on complimentary programs focused on cyber security skills frameworks and career pathways to identify opportunities to collaborate
- Tasmanian Government, 12 May – program briefing and sharing session to inform the panel discussion at the Tasmanian event
- Investment NSW, 31 May – participated in the NSW Cyber Security Skills Framework – industry focus group interview
- ACSC, 28 June – program update, report feedback and discussion about ACSC potential involvement and support in phase 2
- Industry stakeholders
 - UK Government, 4 April – program update and sharing/learning session about UK Council business structure
 - DSO, 11 April – briefing and update on program progress and outcomes
 - Crest, 13 April – program sharing session and explored opportunities to collaborate
 - Hudson, Technology & Projects, 28 April – program sharing session and explored opportunities to collaborate
 - Engineers Australia, 28 April, 26 May, 23 June – ongoing engagement to share and collaborate on respective programs of work to ensure consistency where relevant.
 - Engineers Australia, 11 May & 13 June – program briefing and discussion about how we may work more closely with Engineers Australia in phase 2
 - Lumify Group, 17 May – program sharing session and explored opportunities to collaborate
 - University sector, 23 and 25 May – program briefing and feedback session with Macquarie University, Melbourne University, University of Tasmania, Deakin University, RMIT and Australian Technology Network
 - Fifth Domain, 26 May – program sharing session and explored opportunities to collaborate
 - Australian Women in Security Network (AWSN), 8 June & 21 June – program and research sharing sessions, and explored opportunities to collaborate
 - Insurance Council of Australia, 13 June – program briefing and discussed and agreed how we might work together in phase 2

- Wise Law, 16 June – program sharing session and explored opportunities to collaborate
- Skills Framework for the Information Age (SFIA), 22 June – introduction, sharing session and discussed how we can collaborate in ACSP phase 2 and SFIA 9 consultation
- Australian Cyber Collaboration Centre, 29 June – program sharing session and explored opportunities to collaborate

Program Promotion

Following the public announcement in late March a dedicated [ACSP program website page](#) was created on the AustCyber website to promote the program and co-design team. Five documentary-style videos have been created featuring interview footage with ACSP co-design team participants – one longer in length, and four shorter ones with individual interviews. These have been uploaded to and promoted via AustCyber's various channels. The videos and the media release were added to the relevant sections of the AustCyber website.

Work began in late June drafting ACSP FAQs to feature on the ACSP website page. The co-design team members are involved in the development and final approval of these FAQs. They will be published and promoted in the next reporting period.

A marketing plan began development to raise awareness of the program details, co-design team, stakeholders and plans for the next phase.

s22

S22

S22

S22

S22

s22				
-----	--	--	--	--

	xisting National Node Network contractual arrangements ended

Australian Cyber Security Professionalisation (ACSP) program

Current status overview	Please refer to the detailed ACSP program update under c. Skills building activities above Estimated 100% complete (phase one)
Key activities completed	Delivered co-design team workshop 5 focused on professional

in period (max 5)	recognition body and scheme (part 2) • Produced three detail employer personas - Non technical SMEs, Technical SMEs and Corporates • Delivered draft phase 1 report which included the phase 2 proposal to DISR, Home Affairs and ACSC for feedback • Participated in the Australian Computer Society (ACS) event <i>Building Tasmania's Cyber Security Professionalism</i> held in Hobart on Thursday 26th of May. • Strategically identified and secured new key stakeholders to work with in phase two including two new co-design team members
--------------------------	---

s22

S22

S22

S22

S22

S22

S22

S22

S22

S22

S22