Industry Knowledge Priorities

Approach to developing knowledge priorities

Knowledge priorities have been developed in line with the current and foreseeable needs and opportunities for industry research and commercialisation in the Australian cyber security sector. They will be used to inform AustCyber's activities as it works with industry and the research community to improve research focus, collaboration and commercialisation performance. This includes engaging with stakeholders in existing cyber security focus areas to develop cyber security capabilities in Data61 and the Defence Science and Technology Group, as well as in universities across Australia. AustCyber will use its nationwide networking expertise to work towards maturing Australia's cyber security ecosystem, and also rely on Data61's existing arrangements with Australian universities on research and commercialisation.

These knowledge priorities for the Australian cyber security have been developed based on a literature review of existing research focuses and consultations with stakeholders as part of the development of the Sector Competitiveness Plan. The major documentary sources are the Australian Government's Science and Research Priorities and the CSIRO's report Enabling Australia's Digital Future: cyber security trends and implications.[1]

Industry Knowledge Priorities

1. Emerging prevention, detection and response technologies
    a. Prevention: New ways of supporting the nation's cyber security by discovery and understanding of threats, vulnerabilities and opportunities
        i. Being dynamic and proactive with approaches to identifying vulnerabilities, including tools to better predict malicious actor drivers and behaviour
        ii. Prioritising risks in order maximise the value and impact of prevention efforts
        iii. Classifying these vulnerabilities
            1. Exploitation by malicious actors
            2. Non-malicious events such as natural disasters, equipment failure and human error
        iv. From this, developing national resilience, including
            1. Encryption of data
            2. Distributed storage systems that mitigate the impact of a breach
            3. Improved user behaviour
    b. Detection: Discovering and assessing intrusions
        i. Determining which technologies can be used to discover intrusions, and developing methods to differentiate this activity from normal human/machine behaviour
        ii. Developing methods to detect a breach even if nothing has been affected yet
        iii. Developing technology to increase the frequency of audits without hampering business activities or incurring significant costs
    c. Response: Recovering from a breach
        i. Determining what technologies can be used to remove all known infected systems, applications and devices from the network
        ii. Understanding ways to embed lessons learned for human behaviour and workplace culture
        iii. Increasing the speed at which cyber security breach info is shared across the community
        iv. Ensuring systems continuity, including through self-healing systems
2. Identity, authentication and authorisation in the cyber domain
    a. Finding new strategies and techniques for systems, applications and individuals to verify, identify and establish trust, including understanding the implications of the abuse of trust
    b. Identifying ways to manage the increasing digital access points (and therefore threat vectors) because of trends toward integrated platforms and mobility
    c. Identifying the best use of advanced sensors/intelligent devices to verify trust

[1] https://www.csiro.au/en/Do-business/Futures/Reports/Enabling-Australias-digital-future

3. Ensuring security, privacy, trust and ethical use of emerging technologies and services such as
   a. Cloud computing
   b. Cyber-physical systems, including the Internet of Things, robotics, self-driving cars etc.
   c. Machine learning
   d. Big data and data analytics
   e. Mobile applications
4. Approaches to deal with the increasingly 'shared' responsibility of cyber security
   a. Developing a better understanding of user behaviour at the macro level (including norms of behaviour in cyberspace and user interaction with integrated platforms) and its impact on cyber security
   b. Ensuring the evolution in cyber security policies and skills closely match changes in technology, our adoption and then dependence
   c. Creating a culture with a deeper understanding of cyber security challenges and breaches, including the importance of information sharing, recognising the interdependence of cyber security with national security, national interest and economic prosperity

Sector Challenges

AustCyber invites Expressions of Interest from Australian based organisations to provide a solution against one or more of the challenges that the sector currently faces. These areas of focus are thematically aligned to Australia's Cyber Security Sector Competitiveness Plan, authored by AustCyber. Projects that provide solutions to these areas of focus will make a measurable contribution to the infrastructure required for the sustainable growth of Australia's cyber security sector. All projects must demonstrate secure by design principles and the ability to demonstrate how ongoing cyber resilience can be achieved as part of their solution.

GROW & EXPORT

1. Measuring supply, demand and career pathways to grow Australia's cyber security workforce

Challenge description & context

Cyber security skill and talent gaps exist across Australia, and continues to impact the unrealised economic potential for the cyber security sector. Australia's Cyber Security Sector Competitiveness Plan highlights that while the Australian cyber security workforce is growing, the skills shortage is still severe, needing an additional 18,000 cyber security professionals by 2026. Meeting this demand requires detailed knowledge of the cyber security workforce in each state and territory to inform employers, students, educators, career counsellors, job seekers, current workers as well as policy makers on the many opportunities that exist for workers to start and advance their careers in cyber security.

AustCyber is seeking a digital platform that demonstrates supply and demand for cyber security jobs in each Australian state and territory aligned to the internationally recognised US National Initiative for Cybersecurity Education (NICE) workforce framework. Solutions must also provide a dynamic evidence base to show career pathways to key jobs within cyber security, common transition opportunities between them, and detailed information about the salaries, credentials, and skill-sets associated with each role.

Proposed solutions must at a minimum be able to answer the following questions for users of the platform:

Employers

- How large is the cyber security workforce in my state/territory? How does that compare to other Australian jurisdictions?
- How much does it cost to hire cyber security professionals in my state/territory, by job role?
- How hard will it be to fill a cyber security vacancy in my state/territory? Do I need to source cyber security workers from other parts of the country or via Visa programs?

AustCyber reserves the right to amend the Projects Fund guidelines to which this form relates at any time, where such amendments will comply with the Industry Growth Centres Initiative Programme Guidelines. This document is not a legal contract; it is a set of guidelines to assist applicants with completing AustCyber project applications

Educators and career counsellors

- Against the job roles under the NICE framework, what practical skills should we teach students to prepare them for roles in cyber security? How are these reflected in different courses?
- What education levels do employers require for cyber security workers in my community?
- What entry-level jobs can students target to begin their careers in cyber security?
- What cyber security industry certifications are most in demand at a community level? How do these certifications relate to different roles in the NICE Cyber Security workforce framework?

Students

- Is there strong demand for cyber security jobs in my state/territory?
- What skills and educational credentials are needed to enter a career in cyber security?
- What are the graduate salaries on offer if I work in cyber security?

Job seekers and current workers

- How in-demand are cyber security jobs in at a community level?
- What roles can I target to start my career in cyber security?
- How can I transition between cyber security roles and advance my career?

Policy makers

- How large is the cyber security workforce? How does that compare to other locations?
- How severe is the workforce shortage at a community level?
- What types of cyber security jobs are most in demand in the community?

SCP knowledge priority

This challenge also contributes to the delivery of Industry Knowledge Priorities under Australia's Cyber Security Sector Competitiveness Plan.

3) Ensuring security, privacy, trust and ethical use of emerging technologies and services such as

d) Big data and data analytics

4) Approaches to deal with the increasingly 'shared' responsibility of cyber security

(b) Ensuring the evolution in cyber security policies and skills closely match changes in technology, our adoption and then dependence

2. Mapping capability in Australia's cyber security ecosystem

Challenge description and context

Australia's cyber security sector has the potential to capture a significant share of the growing global cyber security market. Australia's rapidly expanding cyber security sector comprises both foreign owned companies with local offices employing Australians, established Australian companies (including ICT companies now offering customers cyber security services) and an increasing number of Australian cyber security startups and scale-ups with innovative technology and services that represent genuine sovereign capability.

Critical to understanding the depth and breadth of capability of the Australian cyber security ecosystem is the need to catalogue, track and measure the various types of Australian companies, institutions and supporting service providers, and their capability. AustCyber is seeking a digital platform that provides publicly accessible and up to date information on the offering of Australian cyber security companies and their capabilities. The solution will be used by industry, investors, institutions, researchers, and policy makers in addressing cyber security related decisions relevant to their activities, including understanding cyber security trends, the policy environment and competition.

Solutions should seek to answer who and how many cyber security companies, institutions and service providers exist in the Australian ecosystem; an understanding of their capability types, including insights on their growth; and for Australian cyber security companies, their export achievements and international scalability.

SCP knowledge priority

This challenge also contributes to the delivery of Industry Knowledge Priorities under Australia's Cyber Security Sector Competitiveness Plan.

4) Approaches to deal with the increasingly 'shared' responsibility of cyber security

c) Creating a culture with a deeper understanding of cyber security challenges and breaches, including the importance of information sharing, recognising the interdependence of cyber security with national security, national interest and economic prosperity

3. Building cyber capacity in regional/remote areas of Australia

Challenge description and context

Around two thirds of Australia's export earnings come from industries in regional/remote areas such as agriculture, tourism, retail, services and manufacturing. Due to their remote locations, many industries in regional areas have greater reliance on the internet and technology to conduct business, thereby increasing their exposure to cyber security risks. Additionally, the communities that provide services to these sectors often do not have the same awareness of cyber security or access to products, services and training.

AustCyber is seeking expressions of interest for a project that focuses on increasing cyber capacity into regional and remote areas of Australia.

SCP knowledge priority

This challenge also contributes to the delivery of Industry Knowledge Priorities under Australia's Cyber Security Sector Competitiveness Plan.

4) Approaches to deal with the increasingly 'shared' responsibility of cyber security

b) Ensuring the evolution in cyber security policies and skills closely match changes in technology, our adoption and then dependence

4. Navigating federal and state/territory government procurement processes across portfolio requirements

Challenge description and context

Australian Federal and State/Territory governments are collectively the country's single largest procurer of technology based solutions including cyber security. Increasingly, there are matters of national security that require government to procure highly trusted cyber security products and services. Australian cyber security companies are providing unique innovative technical solutions to government agencies, including defence both in Australia and internationally. Ensuring that Australian governments have knowledge of sovereign cyber security capability and access to this capability for procurement decisions is of increasing priority.

However, as the Australian cyber security sector matures, it would benefit from a deeper understanding of procurement and onboarding processes as well as access to real time information on any changes to procurement regulations, policies and procedures many Australian cyber security companies lack the understanding to navigate government procurement processes including the various rules and regulations across jurisdictions and departments. Often, access is unclear and the process is confusing, causing lengthy delays and higher costs.

AustCyber is seeking Expressions of Interest for innovative solutions that can help address this for enabling better matching between Australian cyber security companies and end users in government. Solutions must be scalable, repeatable and measurable.

SCP knowledge priority

This challenge also contributes to the delivery of Industry Knowledge Priorities under Australia’s Cyber Security Sector Competitiveness Plan.

4) Approaches to deal with the increasingly ‘shared’ responsibility of cyber security

a) Developing a better understanding of user behaviour at the macro level (including norms of behaviour in cyberspace and user interaction with integrated platforms) and its impact on cyber security

b) Ensuring the evolution in cyber security policies and skills closely match changes in technology, our adoption and then dependence

c) Creating a culture with a deeper understanding of cyber security challenges and breaches, including the importance of information sharing, recognising the interdependence of cyber security with national security, national interest and economic prosperity

5. Measuring the growth of Australian cyber security ecosystem and its impact on the Australian economy

Challenge description and context

Cyber security is the bedrock of all digital activity, supporting trusted e-commerce, online banking, cloud computing and other, now-ubiquitous business models and services. The growth of cyber security sector and its impact on the Australian economy is poorly understood, in a large part due to a lack of robust and/or credible measurements.

Improving the way we measure the Australian cyber security ecosystem and its impacts on the domestic and international economies will allow governments to form more robust and sophisticated industry development policies; encourage investment in the sector as well as in organisational/enterprise cyber security; and clarify the landscape for cyber security companies that need to understand their commercial surroundings and the opportunities therein.

Through a previously commissioned study on ecosystem measurement activities authored by AustCyber, Australia has developed a framework to measure the growth of the domestic cyber ecosystem sector and its impact on the national economy. We are seeking proposals to value-add and implement this framework.

Using and improving on the framework, solutions should seek to measure the growth of Australia’s cyber security sector, its value add to Australian industry, and the contribution the cyber security ecosystem provides to the whole of economy – in as close to real time as possible as well as over time.

SCP knowledge priority

This challenge also contributes to the delivery of Industry Knowledge Priorities under Australia’s Cyber Security Sector Competitiveness Plan.

4) Approaches to deal with the increasingly ‘shared’ responsibility of cyber security

c) Creating a culture with a deeper understanding of cyber security challenges and breaches, including the importance of information sharing, recognising the interdependence of cyber security with national security, national interest and economic prosperity

EDUCATE

6. Cutting edge training resources for TAFECyber qualifications

Challenge description & context

In January 2018, Australia’s first national skills-based Certificate IV in Cyber Security (22334VIC) and Advanced Diploma in Cyber Security (22445VIC) qualifications were launched under the ‘TAFECyber Initiative’ at Parliament House in Canberra. The qualifications were developed by Box Hill Institute in close collaboration with industry and have been rolled out to TAFECyber providers nationally with the support of AustCyber on behalf of the cyber security industry.

There is now a need to implement a mechanism to support regular updates (at a minimum annual basis) to the training resources used by TAFECyber providers. AustCyber is seeking Expressions of Interest from industry to develop such a mechanism as well as new training resources that demonstrate leading edge training techniques and technology for use at the Certificate IV and Advanced Diploma level. Resources must be accessible to all TAFECyber providers across a common Learning Management System. Approaches to this problem must demonstrate close consultation with TAFECyber providers as well as a cross-sector of Australian industry. Consideration should be given to both online and in person delivery mechanisms of the course.

General information regarding the Technology and Further Education (TAFE), their systems and services can be found at TAFE Directors Australia, https://www.tda.edu.au/

SCP knowledge priority

This challenge also contributes to the delivery of Industry Knowledge Priorities under Australia's Cyber Security Sector Competitiveness Plan.

3) Ensuring security, privacy, trust and ethical use of emerging technologies and services such as:

- Cloud computing
- Cyber-physical systems, including the Internet of Things, robotics, self-driving cars etc.
- Machine learning
- Big data and data analytics
- Mobile applications

7. Networked Training Security Operations Centres (TSOCS) for Australian higher education providers

Challenge description and context

Leading Australian higher education providers of cyber security education and training have implemented Training Security Operations Centres (TSOCs) as a means to enhance practical skills development and real world training simulation that translates to job-ready cyber security professionals for Australian employers. To prevent the emergence of training silos, AustCyber is seeking a technical overlay to enable Australian providers of cyber security education and training involving TSOCs and similar training facilities to be able to inter-connect. Solutions must be vendor agnostic, facilitate joint training, simulation exercises and measurement of skills development aligned to the National Initiative for Cyber Security Education (NICE) workforce framework and be accessible to all public providers of cyber security education and training.

All applications need to ensure that they meet best practice market solutions for SOCs. The infrastructure must have the ability to deliver training to regional and remote areas, and interlink with other Higher Education TSOCs in Australia.

SCP knowledge priority

This challenge also contributes to the delivery of Industry Knowledge Priorities under Australia's Cyber Security Sector Competitiveness Plan.

Approaches to deal with the increasingly 'shared' responsibility of cyber security

a) Developing a better understanding of user behaviour at the macro level (including norms of behaviour in cyberspace and user interaction with integrated platforms) and its impact on cyber security

8. Cyber security challenges for Australian schools

Challenge description and context

Australian school students and teachers have provided extensive positive feedback on the benefit of classroom activities that are automatically marked and directly address the Australian Curriculum: Digital Technologies, particularly those which provide student exposure to authentic cyber security role models.

AustCyber is seeking Expressions of Interest for projects that will build on the highly successful ACA Challenges project. The approach must focus on building comparable Challenges for Primary Schools and Senior Secondary Schools nationally.

SCP knowledge priority

This challenge also contributes to the delivery of Industry Knowledge Priorities under Australia’s Cyber Security Sector Competitiveness Plan.

4) Approaches to deal with the increasingly ‘shared’ responsibility of cyber security

b) Ensuring the evolution in cyber security policies and skills closely match changes in technology, our adoption and then dependence

9. Cyber security challenges platform for all ages

Challenge description and context

Cyber Security Challenges are a practical way for learners of all ages to demonstrate their cyber security aptitude and learn new skills. This is achieved by immersing participants in real-world scenarios that draw out a learner’s aptitude and ability to operate in a cyber security related work role. The gamified format of Cyber Security Challenges includes technical hands-on keyboard as well as non-computer-based competitions. Technical Challenges often involve learners demonstrating their ability to protect against would-be attackers or exploit security vulnerabilities while non-computer-based Challenges can be used to demonstrate a learner’s policy, strategy, legal and business acumen to solve real or simulated cyber security problems facing countries and organisations today.

AustCyber is seeking the development of a Cyber Security Challenges Platform to enable the scaling of existing Australian grass-roots and other challenges traversing the technical and non technical aspects of cyber security. The platform will make Challenges open source for use and will include a “Challenge Generator” providing capability for Challenges to be spun up in a learning environment without the need for repeated deep technical development every time. Fundamentally the platform must provide population level metrics on skills development and gaps mapped to a common workforce framework. Data must also be made available via an API or other mechanism to employers looking for specific skills demonstrated by Challenge participants and as an evidence base for future government policy that aims to close ‘skills gaps’ where and when they emerge.

SCP knowledge priority

This challenge also contributes to the delivery of Industry Knowledge Priorities under Australia’s Cyber Security Sector Competitiveness Plan.

4) Approaches to deal with the increasingly ‘shared’ responsibility of cyber security

b) Ensuring the evolution in cyber security policies and skills closely match changes in technology, our adoption and then dependence

10. Cyber security professional learning for Australian school teachers

Challenges Description and Context

Teacher professional development in both broad cyber awareness and more specialist cyber security education is critical for ensuring that Australian schools and teachers are well prepared to teach the next generation of Australian cyber security professionals. As reported in the National teaching workforce dataset data analysis report 2014, there is a lack of prior experience of our teaching community – only 0.4 per cent of the national teacher workforce have specialist qualifications within ICT, with 13.8 per cent of primary teachers completing a single Computing subject in Year 3 or above of their teacher qualification studies, compared with only 5.9 per cent of secondary teachers.

While there has been significant effort and funding directed towards STEM-based professional learning of recent years, this has been primarily directed towards the fundamentals of the incoming Digital Technologies Curriculum and general ICT capability. AustCyber recognises this challenge and seeks solutions that will provide targeted cyber security teacher professional learning to Australian teachers that provides scalable and sustained access to professional learning support.

Solutions must demonstrate:

- mechanisms to connect industry with teachers to help them deepen their understanding and build strong local support networks for ongoing support
- applicability to both primary and secondary school educators
- close alignment with existing programs of work such as the internationally recognised US National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, ACA Schools Challenges and CyberTaipan.

Data in the problem statement can be referenced to Willett, M., Segal, D., & Walford, W. (2014). National teaching workforce dataset data analysis report 2014. Available at: https://docs.education.gov.au/node/36283. Commonwealth of Australia.
The Challenge has been validated by University of Adelaide, CSIRO, Questacon, Google and Australian Computing Academy.

SCP knowledge priority

This challenge also contributes to the delivery of Industry Knowledge Priorities under Australia's Cyber Security Sector Competitiveness Plan.

4) Approaches to deal with the increasingly 'shared' responsibility of cyber security

b) Ensuring the evolution in cyber security policies and skills closely match changes in technology, our adoption and then dependence

If you have any questions, please email projectsfund@austcyber.com.