AISA Australian Information Security Association

2023-2030 Australian Cyber Security Strategy Response

Context

Background context on Cyber Security in Australia

As the peak body for Cyber Security professionals and the sector, AISA conducted the following in preparation for this response to Government:

1. Roundtable discussions across the nation with business leaders, executives and Chief Information Security Officer (CISO) / Chief Security Officer (CSO) / Chief Information Officer (CIO)s.
2. Townhall discussions with members in WA, SA, VIC, ACT, NSW and QLD.
3. Research across our 10,000+ individual members and our corporate partners to survey their views and opinions.
4. Consultation with AISA's Executive Advisory Board for Cyber which is comprised of over 60 CISO ,CSO and CIOs.

Skills crisis unfolded over decades

For several years, a debate has been ongoing regarding the existence of a cyber security skills crisis across all industries, as well as within the cyber security sector itself. Although some organisations have struggled to find individuals with the necessary skills to fill vacancies, the issue facing the sector is more multifaceted than merely implementing professionalisation, accreditations or investing in additional industry-based training programs.

To fully comprehend and address the problem, we must first explore its origins and propose well-rounded recommendations for resolution. By understanding the origins of the cyber security skills crisis and implementing comprehensive recommendations, we can work towards resolving the issue and building a more robust, skilled, and secure cyber landscape.

To this end, we have consolidated the key aspects of the feedback provided by our members and the following section outlines:

- Challenges within the education system and within the cyber security industry, and
- AISA's recommendations to solve for these challenges.

Challenges within the Tertiary Education System (Supply Side)

Numerous tertiary education institutions, including universities and TAFEs, offer dedicated cyber security courses for both undergraduate (Certificate IV, Diplomas, Bachelors) and postgraduate (Masters and PhD) students. These providers aim to impart fundamental knowledge of cyber security, critical thinking skills, and, in some cases, hands-on experience with prevalent cyber security tools. Additionally, universities typically cover basic research and investigative techniques.

Generally, TAFE institutions emphasise practical learning, such as building networks, applications, systems, and cloud infrastructure, while universities primarily concentrate on theoretical aspects. However, it is worth noting that some universities have begun to adopt a more TAFE-like approach in their curriculum. Key performance indicators (KPIs) for the academic sector, particularly universities, mainly revolve around Category 1 to 4 funding (e.g., the amount of funding a researcher or department attracts from government, industry, or a combination) and the number of research papers published in Q1 journals (i.e., first quartile rated journals based on their performance over the last three or four years), as well as conference paper submissions to highly rated conferences.

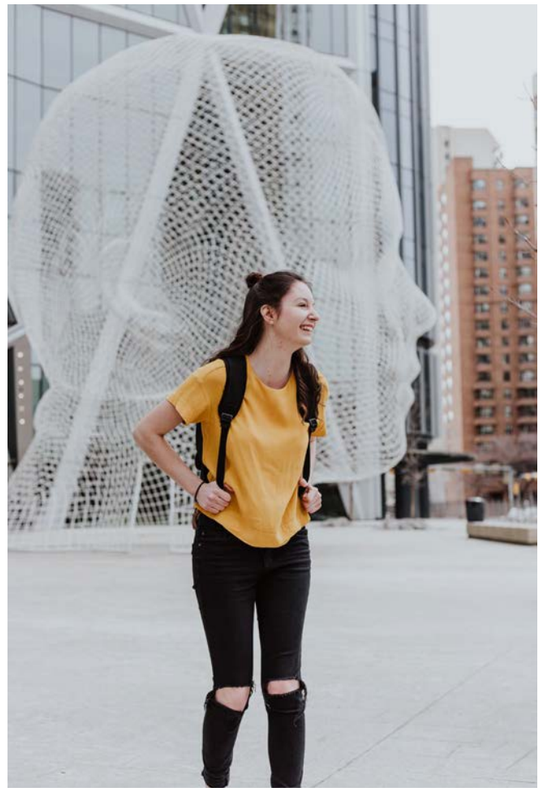
There are no measurable KPIs centred around student outcomes or the number of students who secure meaningful employment based on their university studies. Consequently, the primary focus at most universities is academic research output and maximising both local and international student enrolments, often without considering the value of the course as a pathway to meaningful employment. Several factors compound the challenges facing cyber security education, including:

- **Poor course certification:** Cyber security courses are certified by organisations that lack expertise in the field, do not represent the sector, and fail to ensure that courses lead to meaningful employment for students.
- **Limited interdisciplinary education:** Courses often fall under Information Technology or Business schools, faculties, or colleges, and are rarely shared between the two. This leads to an imbalance in focus, with IT-centric courses neglecting policy, regulatory, legal, risk, or business aspects of cyber security, and business-focused courses lacking in-depth technical knowledge. Internal politics surrounding revenue recognition often prevent collaboration between schools, faculties, or colleges.

  Cyber security is a multidisciplinary field that involves not only technical expertise but also understanding of human behaviour, business processes, and legal and ethical considerations. Tertiary institutions do not offer sufficient interdisciplinary education that encourages students to develop a comprehensive understanding of cyber security from multiple perspectives.

  Industry recommends courses should be re-engineered to be based on the disciplines inside cyber security e.g. Testing and Assurance, GRC, Forensics, Incident Response, IDAM, leadership etc. Tertiary providers could provide a common first year for cyber security fundamentals with multiple pathways for later years to specialise.
- **Skill challenges of educators:** The tertiary sector struggles to find skilled and qualified educators to teach cyber security-related subjects. Many university educators have not worked in the industry or government, and lack understanding of the pressures, challenges, threats, and risks faced by these organisations. Attracting and retaining industry talent is difficult due to lower pay scales in tertiary education compared to industry or government, and a culture that prioritises research output over student education. This often leads junior staff with higher teaching loads as compared to professors.
- **Insufficient collaboration with industry:** There can be a lack of strong partnerships between tertiary institutions and industry stakeholders, leading to a disconnect between the skills and knowledge being taught and the actual needs of employers. Greater collaboration between academia and industry can help ensure that curricula are tailored to address real-world challenges and produce job-ready graduates.
- **Outdated curricula:** University and TAFE courses typically undergo major updates every four to five years, which is not frequent enough to keep pace with the rapid changes in cyber security legislation, regulation, policy, technology, and adversary tactics. As a result, students may be taught outdated information. While educators can update their subjects at any time, there is little reward for doing so, and the responsibility falls on individual educators driven by a desire to ensure the best outcomes for students. However, there have been some positive developments, such as the recent update to the Certificate IV in Cyber Security.

  The original course focused primarily on producing Security Operation Centre (SOC) Analysts, neglecting policy, risk management, and cloud cyber security. The updated 2023 course structure, which prepares students to become Cyber Security Technicians, is more closely aligned with industry needs. This change is crucial as the SOC Analyst role has shifted due to technological advances, necessitating higher-level skills for meaningful job opportunities for those completing the Certificate IV in Cyber Security.
- **Overemphasis on certifications:** While professional industry certifications can be valuable, an overemphasis on obtaining certifications can lead students to focus on passing exams rather than developing a deep understanding of cyber security principles and practical skills. It also distorts the market where certifications become an employment benchmark rather than the more important aspects of aptitude, attitude and hands on work experience.



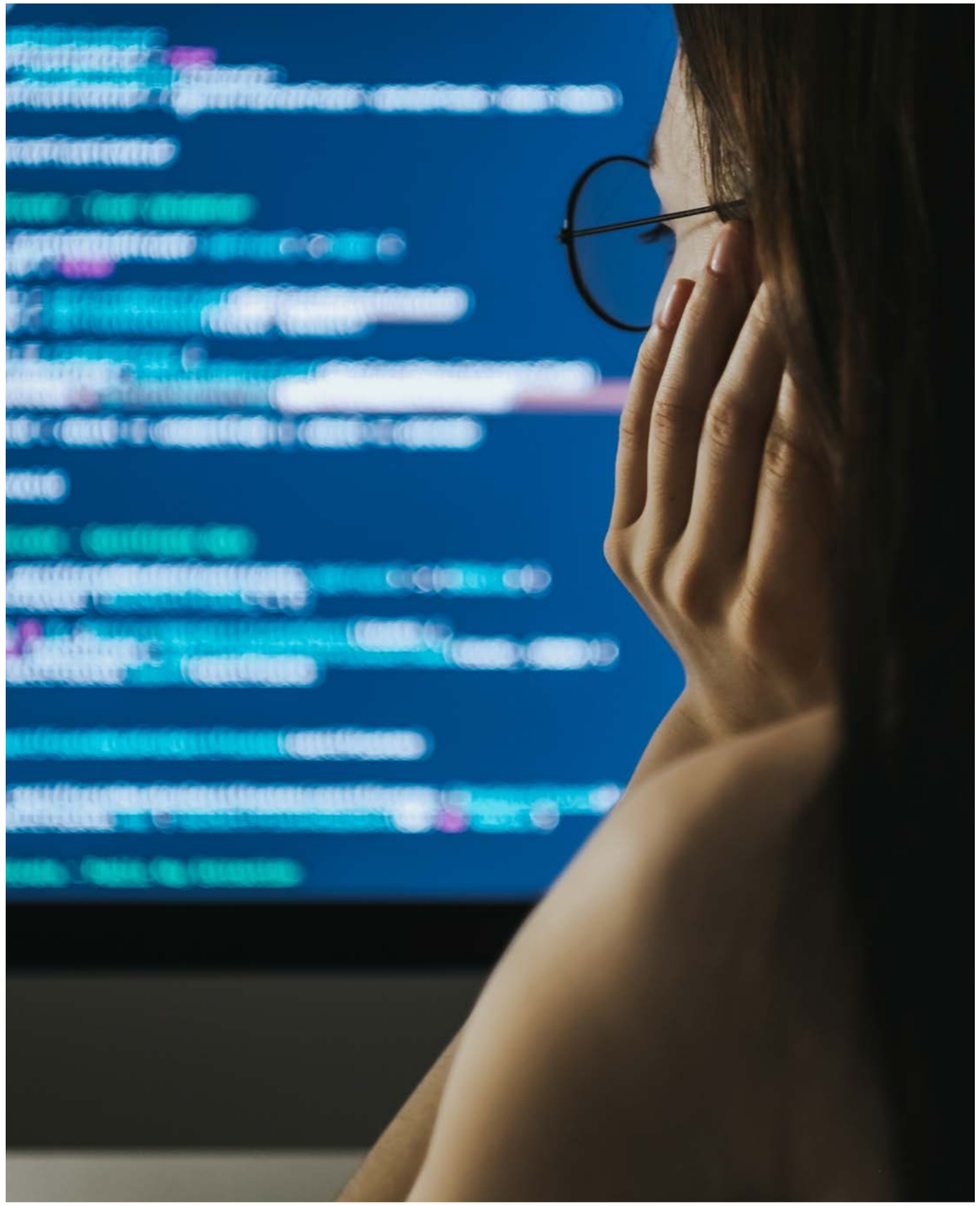
- **Lack of diversity:** The cyber security field suffers from a lack of diversity, with underrepresentation of women and minority groups. This can limit the range of perspectives and ideas in the field, and hinder the development of innovative solutions to cyber security challenges.

- **Inadequate resources:** Tertiary institutions may lack the necessary resources, such as state-of-the-art labs, equipment, and software, to provide students with a cutting-edge education in cyber security. This can hinder their ability to stay current with the latest developments in the field.

- **Insufficient practical experience and industry placement opportunities:** While many tertiary institutions emphasise theoretical and fundamental knowledge, they do not offer enough hands-on experience, internships, or industry projects for students. This gap in real-world experience can leave graduates inadequately prepared for the workforce. Some courses do provide optional subjects that include unpaid industry work experience or paid placements (approximately $900 per week to the student) lasting several months.

Nearly two-thirds of students participating in paid placements secure meaningful employment with their host organisation upon graduation. However, it is worth noting that many students choose not to pursue paid placements, as the placements extends their studies by three to twelve months. Universities also face challenges in securing paid placements within the industry, and many organisations are unaware of the cost and tax benefits associated with offering such placements. In one case, students at a major bank had to accept paid placements through an intermediary job agency so they would be classified as contractors instead of full-time staff, avoiding any negative impact on the bank's limitations regarding onboarding new full-time employees.

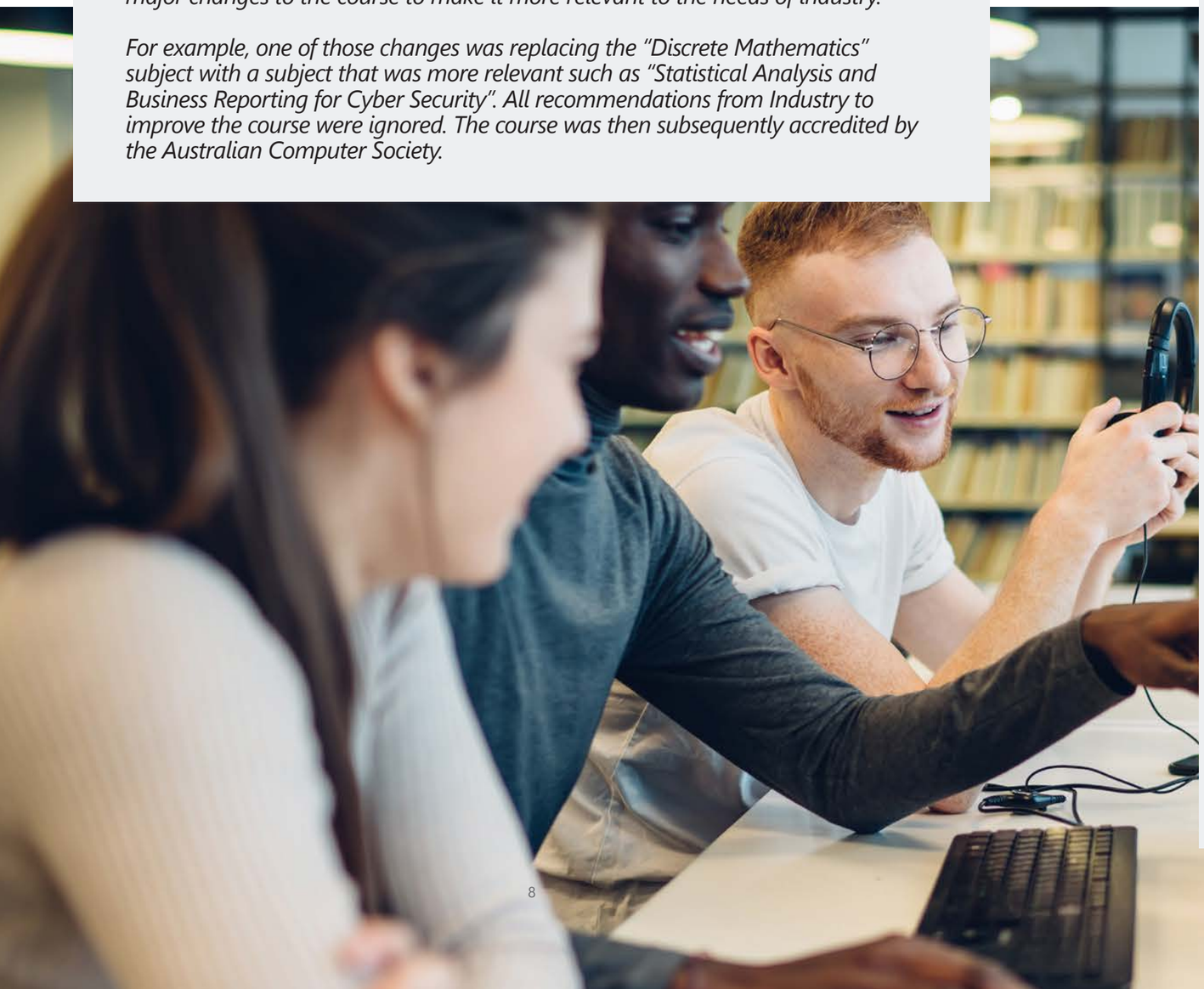
- **Lack of transparent and updated course rankings:** Currently there is no way for consumers to review and compare cyber security courses and match them against their career pathways into cyber security or to evaluate the number of students who gain employment at graduation. There is a need for consumers to have a centralised platform that ranks and rates all cyber security courses in Australia. By ranking and rating courses based on factors such as course content, industry relevance, and graduate outcomes, the platform could incentivise institutions to continuously improve their programs and maintain high standards of education. A centralised platform would offer increased transparency about the quality and relevance of different courses, making it easier for students to compare programs and identify those that offer the best value for their investment in education. A platform that showcases a wide range of courses could help promote diversity in the field by highlighting programs that cater to students with different backgrounds, interests, and learning styles. In addition, a centralised platform would provide students with comprehensive information about various cyber security courses, allowing them to make more informed decisions about which program best aligns with their career goals and interests.



Case Study 1

One of Australia's top University providers for the Bachelor of Cyber Security asked 30+ CISO / CIOs to review their course. Industry CISO / CIOs rated the course very low as it lacked subjects that dealt with legislation, risk management, policy and relevant technical fundamentals for cyber security. CISO / CIOs recommended major changes to the course to make it more relevant to the needs of industry.

For example, one of those changes was replacing the "Discrete Mathematics" subject with a subject that was more relevant such as "Statistical Analysis and Business Reporting for Cyber Security". All recommendations from Industry to improve the course were ignored. The course was then subsequently accredited by the Australian Computer Society.



Case Study 2

Student's perspective of the course:

"I acquired a taste for cyber security after hearing many stories from my father who is a CISO and had been employed in the cyber security industry for approximately 20 years. It sounded like an interesting and rewarding career so when I finished Year 12, I successfully applied for the Double Degree - Cyber Security and Criminology at a leading university. I started the course enthusiastically and unfortunately left it 18 months later totally disillusioned. The industry that I had been told about so many times by my dad, unfortunately did not match the Cyber Security course delivered to me by the University. I was expecting to learn about real life security tasks such as Security Awareness, Security Operations, Security Applications, Security Reporting, Board representation, Data breaches, Incident Response etc. This is a quick summation of the security subjects I endured:

- *Introduction to programming - was a mandatory subject which I, and my father, saw no relevance whatsoever with my Cyber Security career pathway.*
- *Discrete Mathematics - was also a mandatory subject I had to do which is not typically used in Cyber Security.*
- *Computer Systems - which had very little real relevance to Cyber Security and seemed to be a rebranded IT subject.*

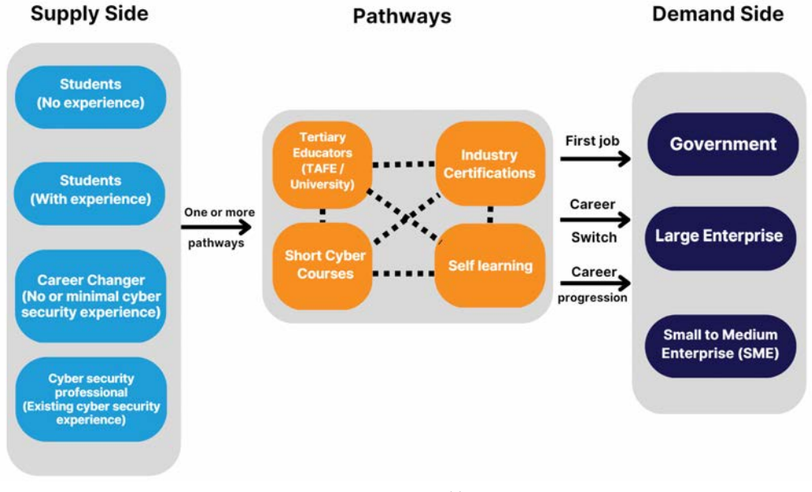
I did enjoy 'Real World Practices for Cyber Security' which reflected what I had gleaned previously about the cyber security industry through research and from my dad's stories. When I then reviewed the remaining subjects, in particular Object Oriented Development, Secure Coding etc, I realised that the structure of the course did not reflect real world practices for my career pathway and unfortunately I withdrew from the course. Without sounding overly critical, I wasn't too impressed with the teaching staff either. Despite one or two exceptions, they weren't very helpful, nor did they have an understanding of real-world issues."

"The structure of the course did not reflect real world practices for my career pathway"

Challenges within industry (Demand Side)

There are several challenges within industry (demand side) when it comes to finding appropriately skilled cyber security professionals. These include:

- **Rapidly evolving landscape:** The cyber security field is constantly changing, with new threats, technologies, and regulations emerging all the time. This dynamic landscape makes it difficult for organisations to identify professionals with up-to-date skills and knowledge.
- **Education gaps:** There are serious gaps in tertiary education and these gaps can make it challenging for organisations to find professionals with the right combination of technical, analytical, and soft skills needed to address various cyber security challenges
- **Experience requirements:** Many organisations seek experienced cyber security professionals who can hit the ground running. This preference for experienced candidates can make it difficult for recent graduates or those with limited work experience to break into the field, especially if they completed courses which lack any work experience or industry placements.
- **Overemphasis on certifications:** With over 460 industry cyber security certifications and the volume of applicants looking for roles; recruiters and HR departments are using industry certifications as a mechanism to cull applicants, potentially missing applicants without certifications who may be suited to the role.
- **Limited awareness of available talent:** Some organisations may not be aware of the full range of talent available in the market, including those who have acquired their skills through non-traditional pathways, such as self-learning, online courses, or boot camps.
- **Inadequate talent pipelines:** Organisations can struggle to build and maintain talent pipelines that can identify and recruit skilled cyber security professionals in a timely manner.
- **Geographical constraints:** The demand for cyber security professionals is often concentrated in certain geographical regions, which can make it difficult for organisations in less-populated areas to attract and retain top talent. With the new Work From Home (WFH) model there is potential to now recruit from regional and rural areas.
- **Diversity challenges:** The cyber security field has historically been less diverse than other industries, which can limit the pool of available talent and hinder organisations' ability to develop creative solutions to complex security problems.
- **International students:** Businesses may be hesitant to employ international students due to visa and work permit restrictions, potential language barriers, or cultural differences that could impact team dynamics. Moreover, the uncertainty surrounding regulatory changes and immigration policies can make it difficult for organisations to plan for long-term talent acquisition and retention of international students from Australian Universities.
- **Time and resource constraints:** Businesses often face time and resource constraints, which can affect their ability to provide adequate training, mentoring, and coaching to new graduates. This can result in less productivity and increased stress for existing employees who must manage and mentor new hires while still fulfilling their own job responsibilities. Furthermore, organisations may find it challenging to allocate resources for professional development or upskilling programs that help bridge the skill gap between fresh graduates and experienced professionals.
- **FTE constraints:** Organisations often have limitations on the number of full-time employees they can hire, which can restrict their ability to bring in new cyber security professionals via University WIL (Work Integrated Learning) programs which includes paid placements.
- **Review and revise job descriptions:** Organisations should ensure their job postings accurately reflect the actual requirements and responsibilities of the position. This includes aligning expectations for entry-level positions with the experience and skills that can reasonably be expected from recent graduates or those new to the field. Many graduates disengage from the sector when entry level job adverts require a minimum of two years of experience or industry certification like CISSP which takes five years of work experience to achieve. It is worth considering that there are challenges how different diversities may read a job description and how it is written could rule people in or out from applying.



Recommendations from AISA on the supply side:

- **Recruit talent from industry:** Tertiary education providers should actively engage industry CISOs and CIOs to enhance their courses and draw on the extensive talent within the sector for teaching various subjects. Many cyber security experts with over 20 years of experience are eager to give back to the community and sector, and this could be one formally recognised mechanism through industry or adjunct professorships. Another channel to bring industry experts and education system closer is by awarding industry experts undergraduate degrees in specialised subjects and encouraging them to share their knowledge from the industry.
- **Placements for educators in industry:** Teachers in tertiary education should be provided with industry secondment opportunities to gain real-world experience in industry or government departments, or both.
- **Uplift staff industry skills:** While adopting vendor-neutral industry certifications may lead to artificial benchmarks that may or may not be suitable, the experience gained from educators obtaining certifications such as CISM, CISSP, or equivalent significantly increases the diverse knowledge and reputation of those educators.
- **Deliver multidisciplinary courses:** Courses should deliver value for students and align with the demand of industry. Courses should be comprehensive and enable students to select technical, non-technical and leadership career pathways in cyber security.
- **Track and report on metrics:** The TAFE and Universities should adopt metrics for tracking and reporting to continually evaluate value of the courses that are being provided. These measures could be
  1) Percentage of intern placements during the course to gain experience,
  2) How may graduates were employed in the cyber security field 6 months after graduating.

Recommendations from AISA on the demand side:

- **Emphasise potential for growth:** Instead of focusing solely on specific qualifications or years of experience, organisations should emphasise the potential for growth and learning within the position. This can attract motivated candidates who may not yet have the desired level of experience, but are eager to develop their skills on the job. Also, shifting focus towards soft-skills and attitude could assist significantly. Unfortunately, organisations need staff capacity numbers to be sufficient to enable new recruits time to upskill.
- **Offer training and certification support:** To attract and retain talent, organisations can provide support for employees to obtain relevant certifications, such as CISSP. This may involve offering financial assistance, study resources, or allocating time for employees to pursue these certifications as part of their professional development.
- **Focus on transferable skills:** In evaluating candidates, organisations should consider transferable skills that may be applicable to cyber security roles. This can help identify candidates who may not have direct experience in the field but possess skills that can be adapted to the specific requirements of the position. Again, this requires a mature HR process and additional time and effort to conduct recruitment in this manner.
- **Implement talent development programs:** Organisations can invest in initiatives that foster talent development, such as internal training programs, mentorship opportunities, and partnerships with educational institutions. This can help bridge the gap between entry-level candidates' skills and the organisation's needs.
- **Track and report:** Like TAFE and Universities, employers should adopt tracking and reporting on statistics about graduates and freshers recruitment, an example could be, after gaining employment post a degree or course how many maintained their initial employment 12 months after degree. Another one that is worth quoting is how valuable the employer found the candidate who was hired post a degree or a course.

Recommendations from AISA for government:

- **Transparent reporting on all cyber security courses:**
  A comprehensive expert panel, comprising CISOs and CIOs from various sectors, should review all cyber security tertiary courses. These courses should be ranked and rated based on relevance and student outcomes for meaningful employment in cyber security. The course rankings should be published on a website, allowing consumers to select the most appropriate course. Each ranked and rated course should indicate the career pathway it is best suited for, enabling consumers to make informed choices. This competitive ranking would drive better competition among tertiary providers, ensuring their courses are relevant and well-matched to the selected career pathways while providing consumers with greater transparency and a way to compare courses.

- **Incentives for business:**
  Promote secondment opportunities for tertiary educators to learn skills from businesses and provide incentives for industry to create WIL placements to ensure students gain paid work experience in the last year of their studies. These initiatives should be supported with appropriate awareness within the sector for organisations to take benefit of these schemes.

ACSC and JCSC Performance

While AISA acknowledges the positive work conducted by the Australian Cyber Security Centre (ACSC) in protecting Australians, questions are raised by businesses, CISO/CSOs and the broader sector on the effectiveness of the ACSC and also the Joint Cyber Security Centre (JCSC). There are several recommendations based on feedback from the sector:

- **Timeliness of threat advice:** The role of the ACSC in advising sectors and critical organisations is of great importance to keeping Australia safe. However, there are several cases where the commercial / private sector has reported alerts and discovery of sensitive material on the dark web faster and more accurately, with the ACSC reporting to the impacted organisation one week post notification by multiple commercial entities.

  Recommendation: ACSC is allocated additional resources to bring the level of notification to sectors up to the same level or better than private / commercial organisations.

- **ACSC material not appropriate for general sectors:** While the ACSC does produce several good advisory documents, frameworks and advice, it is often tailored to larger commercial entities and government agencies. An example of this is the Essential 8 which is of high value for government and defence departments to secure the data and services they manage, but is not appropriate for the Small to Medium Enterprises (SMEs) or the Not-For-Profit (NFP) sector in both type of information, tone and format. AISA is working with COSBOA (Council of Small Business Organisations Australia) and AICD (Australian Institute of Company Directors) to build an Essential 8 Small Business and NFP Edition. This SME / NFP focused Essential 8 will be focused on simple technical controls, cloud based services and culture to drive long lasting behaviour change.

  Recommendation: ACSC works with AISA on the Essential 8 Small Business & NFP edition.

- **JCSCs not providing value for investment:** Prior to the pandemic there was a review conducted into the effectiveness of the JCSCs. Post pandemic, many in the cyber security community have gained little value through the JCSCs. This is also exacerbated by the Work From Home (WFM) model of post pandemic working, with many organisations only having staff attending head offices located in major CBDs two to three days per week.

  Recommendation: Release the review of the JCSCs that was conducted prior to the pandemic for transparency and to better understand what were identified as common challenges with the various JCSCs across the country. Consider alternative ways to improve usability and accessibility of the various JCSCs to justify the large capital expenditure.

1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

It is important to take a reflective approach and build upon the successes of the previous strategy while addressing any shortcomings. Conducting a maturity assessment and defining what it means to be the most cyber secure nation can provide a roadmap for prioritising key areas for improvement.
The best practice approach to national cyber strategy development should be based on conducting a **maturity assessment and implementing a roadmap** based on research and evidence, can be a valuable method for developing an effective cyber security strategy. This approach allows for a wide and tested stakeholder engagement process, involving government, industry, and civil society, which can provide a holistic view of the challenges and opportunities in national cyber security.

AISA in its submission is incorporating inputs from roundtables, town halls, and member surveys to ensure that diverse perspectives are considered in the development of the strategy.

Objective-driven approach with clear metrics for measurement can help in setting achievable and measurable success criteria, which can provide a framework for evaluating the effectiveness of the strategy over time. It is important to approach the development of a new national cyber security strategy with a comprehensive and inclusive approach, considering inputs from various stakeholders and using evidence-based methods for analysis. By building upon the successes of the previous strategy, addressing shortcomings, and setting clear objectives with measurable metrics, the new strategy can be better positioned to effectively address the challenges and opportunities in national cyber security.

The last cyber security strategy called for action from government, businesses, and the community, including a **fourth pillar of professionals** in the new national cyber strategy is a valuable recommendation. Cyber security professionals play a crucial role in safeguarding the nation's digital assets and infrastructure, and their expertise can contribute significantly to strengthening the cyber security sector.

Identifying key themes for the contribution of cyber practitioners can further enhance the effectiveness of the strategy. This could include areas such as capacity building, skill development, knowledge sharing, research, and development, and fostering innovation in the cyber security field. Cyber security professionals can also provide insights on emerging threats, technological advancements, and best practices, which can inform policy decisions and strategic initiatives.

Engaging cyber practitioners in the national cyber strategy can foster a collaborative approach involving government, businesses, communities, and professionals working together towards a common goal of enhancing cyber security. This can create a sense of ownership and accountability among cyber practitioners, encouraging them to actively contribute to nation-building efforts in the cyber security domain.

The cyber security community acknowledges, more needs to be done to better support and enable small to medium-sized enterprises (SMEs). SMEs play a critical role in the Australian economy, contributing almost 50% of the GDP.

Recognising their importance, it is essential to prioritise cyber security measures to protect their digital assets and operations.

The new national cyber strategy should consider the unique challenges and needs of SMEs and provide targeted support to enable them to enhance their cyber security posture. This could include measures such as:

- Financial incentives: SMEs may face budget constraints in investing in cyber security. The strategy could include provisions for financial incentives, such as tax credits, grants, or subsidies, to encourage SMEs to invest in cyber security technologies and solutions.
- Awareness and education: SMEs may lack awareness about the importance of cyber security and the potential risks they face.
- Access to resources: SMEs may have limited access to cyber security expertise and resources. The strategy could facilitate partnerships between SMEs and cyber security professionals or organisations to provide affordable cyber security services, tools, and resources tailored for SMEs.
- Information sharing and collaboration: SMEs can benefit from information sharing and collaboration with other businesses and organisations. The strategy could encourage the establishment of information-sharing platforms, industry-specific forums, or networks to facilitate SMEs in sharing cyber security insights, challenges, and best practices.
- Compliance and regulatory support: SMEs may struggle with complying with current complex cyber security regulations. The strategy could provide guidance and support in understanding and meeting compliance requirements and simplify regulatory processes for SMEs.

By addressing the specific needs of SMEs in the national cyber strategy, Australia can strengthen the overall cyber security landscape by empowering a significant portion of its economy to better protect against cyber threats.

A **risk-based approach** can provide a strategic and systematic framework for governments, industry, and the community to understand the gravity of cyber security issues, prioritise efforts, and collaborate effectively in addressing cyber security challenges. It can help ensure that resources and efforts are directed where they are most needed, and that cyber security strategies and initiatives are continuously reviewed and updated to effectively address the changing threat landscape. Different types of cyber security risks may have varying levels of concern and impact depending on the sector and industry. Small to medium-sized businesses may be more vulnerable to criminal state risks, such as cybercrime activities carried out by organised criminal groups. On the other hand, federal and state governments and defence agencies may be more concerned about national state risks, such as cyber-attacks carried out by nation-states or state-sponsored actors, due to the potential impact on national security, defence capabilities, and sensitive information.

Therefore, it is important to tailor cyber security efforts and strategies to address the specific risks and challenges faced by different sectors and industries. By understanding the specific risks and challenges faced by different stakeholders, cyber security strategies and initiatives can be tailored to effectively address those concerns and enhance overall cyber security resilience clearly identifying areas of responsibilities.

2. What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

a) What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?
A combination of legislation, regulation, and regulatory guidance to improve awareness. Each mechanism has its advantages and limitations, and a comprehensive approach may involve a mix of these approaches to effectively drive cyber security alertness across the board to improve the operational standards within the economy. Ensuring a balance between establishing clear obligations, flexibility, and the practicalities of organisations adjusting to change must be considered, especially when driving improvements across different sectors and industries of varying maturity. Stakeholder engagement, consultation, and ongoing monitoring and evaluation would be crucial in ensuring the effectiveness of the right combination of the reforms.

b) Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?
Customer data and systems are the crown jewels that are the target of any cyber-attack or data breach, so they must be protected. However, this must be done in context to the risk associated with these assets and what value they hold for adversaries. Any further reforms to the SOCI should consider including the evolving threat landscape, technological advancements, and lessons learned from the implementation of the existing Act. It's important to take a reflective approach and build upon enhancing the protection of critical infrastructure in Australia from cyber threats and other security risks.

c) Should the obligations of company directors specifically address cyber security risks and consequences?
The suggestion to introduce direct obligations for company directors and encourage changes to the Corporations Act to explicitly include cyber security responsibilities for boards of directors is in line with the growing recognition of the importance of cyber security at the board level. The cyber security sector strongly supports this change. Cyber security is no longer just an IT issue, but a strategic business risk that requires board-level oversight and accountability, similar to OH&S challenges 30 years ago.

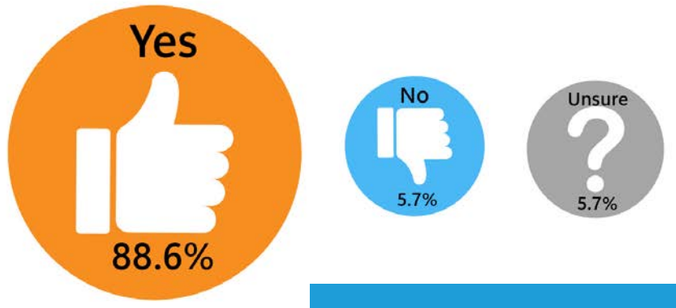
Introducing specific cyber security responsibilities for directors in the Corporations Act will help ensure boards are actively engaged in overseeing and managing cyber security risks, and that cyber security is integrated into the corporate governance framework of organisations. This can help drive a culture of cyber security awareness, behaviour change and accountability at the highest level of decision-making within organisations.

Standard metrics for cyber security responsibilities, like those for financial obligations, can provide a consistent framework for evaluating and reporting on cyber security performance.

These metrics can help boards assess the effectiveness of their organisation's cyber security measures and track progress over time, enabling better risk management and decision-making.

Mandating cyber skills on company boards, at least for publicly listed organisations, would bring expertise and knowledge to the boardroom to deal with the new digital age businesses are expected to operate in and ensure cyber security / privacy related risks are considered in strategic decision-making. Cyber security is a complex and rapidly evolving field, and having directors, or at the very least committees, reporting to the board with relevant cyber skills would enhance the board's ability to understand and effectively address the related business risks. Defining what board reports on cyber security should look like can provide guidance to boards on the necessary information to include in their reporting, ensuring that cyber security matters are clearly articulated and appropriately addressed. This can help improve communication and reporting on cyber security risks and measures, both within the organisation and to external stakeholders.

Changes to the Corporations Act to include cyber security responsibilities for boards of directors



When working with board directors and executives, only 82% were in favour of company director obligations specifically addressing cyber security risks and consequences, while 12% were not in favour and 6% were unsure. Cyber security professionals dealing with governance, risk and compliance were over 92% in favour and only 3.4% against these changes.

88.6% of respondents are in favour of changes to the Corporations Act to include cyber security responsibilities for boards of directors, while only **5.7%** are not in favour and **5.7%** are unsure.

This supports the recommendation to mandate cyber security responsibilities for boards of directors and introduce standard metrics and reporting requirements to ensure that cyber security is effectively integrated into the corporate governance framework of organisations just like other major challenges boards deal with.

d) Should Australia consider a Cyber Security Act, and what should this include?
There is strong support for the creation of a Cyber Security Act, with 87.7% of the cyber security industry and business leaders in favour. This significant support indicates a recognition within the sector and within businesses that comprehensive legislation to address cyber security challenges may be required, but for it to be contained in a single act to improve understanding and compliance. It is interesting to note that the highest support for a Cyber Security Act is within the academic cyber security community, followed by cyber security professionals and business professionals. Board directors and executive leaders, while they still overwhelming support a Cyber Security Act, support is lower at only 83%. Only 4.8% are not in favour of a single Act with 7.5% unsure.

A Cyber Security Act could provide a combined regulatory framework to establish clear guidelines, requirements, and responsibilities for organisations, government agencies, and individuals to effectively manage and mitigate cyber security risks. It could outline standards, best practices, and enforcement mechanisms to ensure that cyber security is prioritised across different sectors of the economy, and that appropriate measures are in place to protect critical infrastructure, sensitive data, and national security interests.

The strong support for a Cyber Security Act among cyber security professionals and board directors/C-suite leaders suggests that there is a recognition of the need for a comprehensive approach to cyber security, beyond voluntary measures or industry standards. It is important to carefully consider the design and implementation of any proposed Cyber Security Act to

ensure that it is practical, effective, and aligned with the needs and challenges of the business environment and adapts to technology changes. Engaging with stakeholders, including peak bodies, cyber security professionals, board directors, and C-suite leaders, can help shape the content and scope of such legislation to ensure that it is comprehensive, relevant, and capable of driving positive change in the cyber security posture of the nation.

The proposal to make the Cyber Security Act simple, with reduced regulatory burden and as a single legislative document, is in line with the need for practical and effective cyber security regulation. Simplifying the regulatory requirements can help organisations better understand and comply with their obligations, while reducing unnecessary administrative burdens that may hinder their ability to implement effective cyber security measures. By consolidating relevant cyber security and privacy requirements under the same Act, it could also provide a streamlined and cohesive approach to addressing cyber security and privacy concerns, recognising the inherent interlinkage between the two.

The recent spate of major data breaches has highlighted the critical importance of cyber security and privacy as interconnected issues that business needs to address. Cyber-attacks often target sensitive personal information, and organisations need to have robust measures in place to protect both the security and privacy of such data. Consolidating cyber security and privacy requirements under the same Act will promote a holistic and coordinated approach to addressing these issues, as organisations would need to consider both aspects together in their compliance efforts, however considering the Privacy Act is currently undergoing a review it may be more appropriate to have a standalone Cyber Security Act.

It is crucial to ensure that any proposed changes and associated legislation are carefully designed and aligned with the evolving cyber security and privacy landscape, and other cyber related regulatory provisions in various acts are removed. This may involve engaging with relevant stakeholders, including organisations like AISA, government agencies, privacy advocates, and other experts in the field, to ensure that the regulatory framework is effective, practical, and capable of addressing the ever-changing cyber security threats and privacy concerns.

e) How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

This may involve engaging with relevant stakeholders, including organisations like AISA, government agencies, privacy advocates, and other experts in the field, to ensure that the regulatory framework is effective, practical, and is not a burden on businesses to implement, seek skills or to be compliant.

f) Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by:

(a) victims of cybercrime; and/or
(b) insurers? If so, under what circumstances?

AISA asked its members if the Government should prohibit individual victims of cybercrime from paying ransomware and extortion demands, and the response to this question was received with some mixed opinions – 42.2% are in support, 23.7% said they were unsure, whereas 34.1% were not in support.

We also asked in the survey if the businesses who are victims of cybercrime should be prohibited from paying ransomware demands, and 54.1% of the respondents are in support whereas 26.5% said "No" and 19.4% were unsure.

Similarly, when asking if the insurers be prohibited from paying for ransomware – 50.8% are in support and 29.4% respondents opted "No" as a response.

What is interesting to note here is that for both businesses and insurers, over 50% of the board directors and C-Suite leaders are in favour of prohibiting ransom payments for cyber crime.

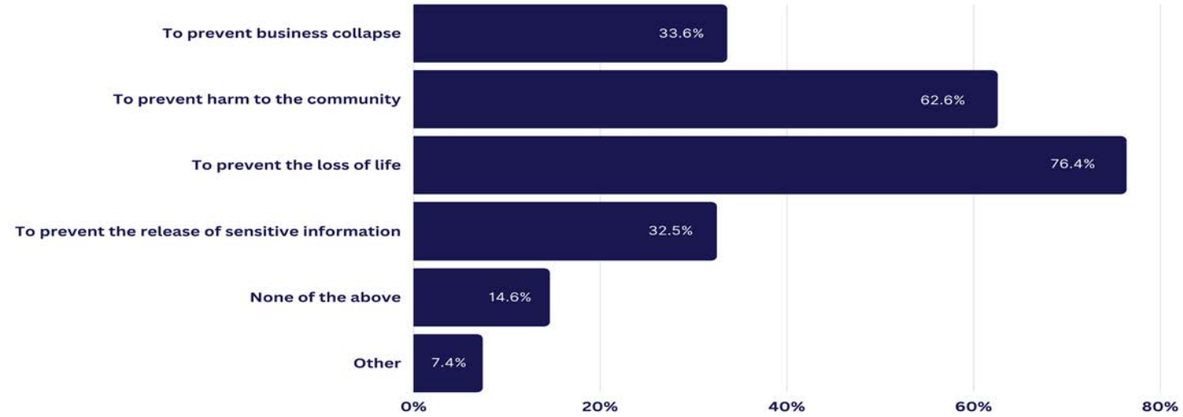
It is also interesting to see from the survey of the sector that 25.5% believe there is value for money in cyber security insurance, whereas 41.7% are 'Unsure' and 32.8% said they don't see value for money in insuring for cyber security.

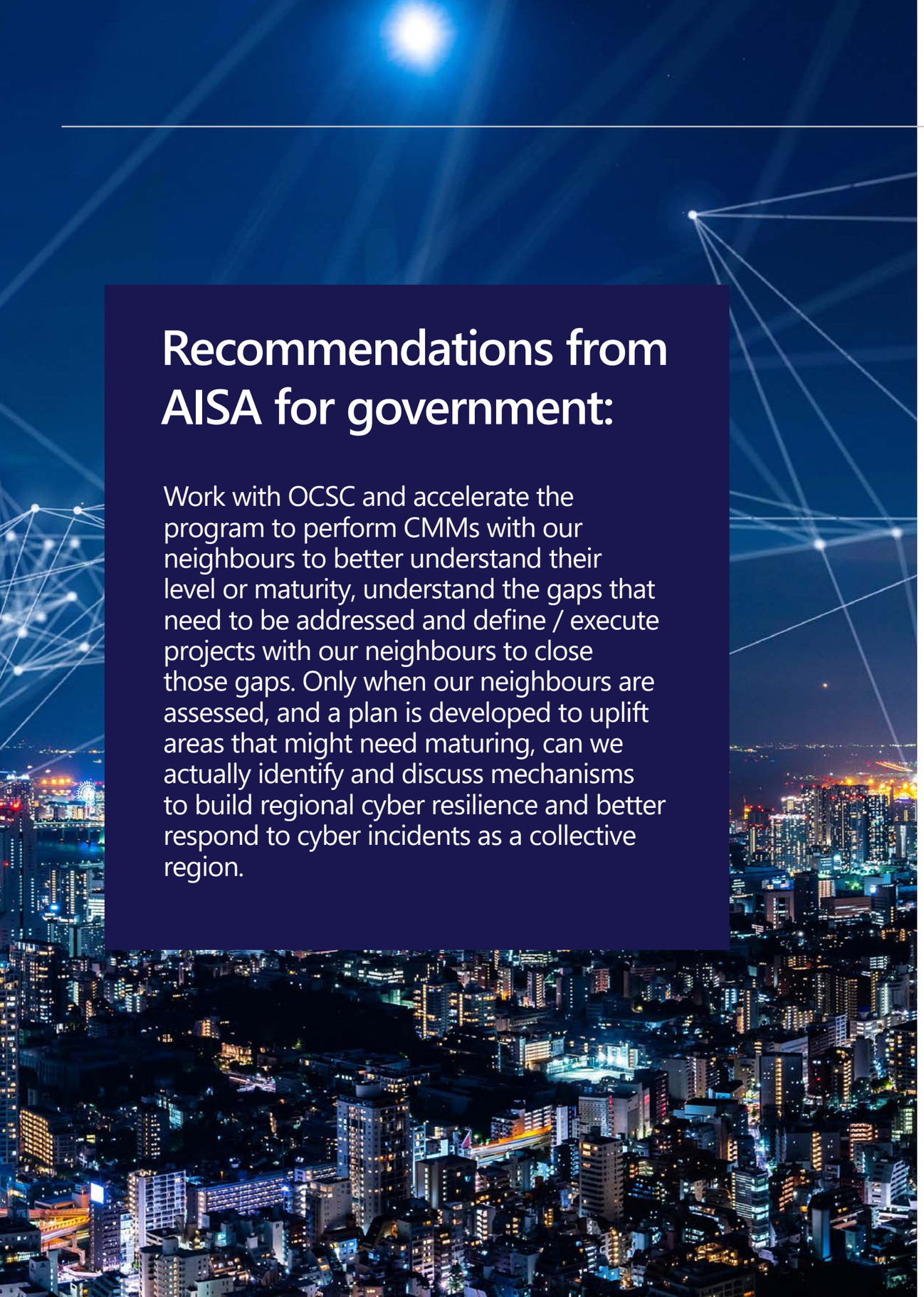
g.) Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

Yes, navigating the complexities of ransomware incidents can be challenging for organisations. Having guiding principles can provide a framework for decision-making in such situations, and government agencies should be part of the decision making too. While the industry view may be divided, it is essential to consider various factors, including the context of the situation and the assets at stake, when dealing with ransom scenarios. There could be various factors affecting the determination an organisation has to make in a challenging situation like ransomware crimes, such as: compliance with applicable laws and regulations, protection of critical assets and systems, risk assessment and business impact, or prevention of further victimisation.

It is crucial to note that every ransomware incident is unique, and decisions should be made on a case-by-case basis, considering the specific circumstances and risks involved. Assistance from governments and different agencies like ACSC can provide valuable insights and guidance in making informed decisions when dealing with ransomware incidents.

Under what special conditions should the government allow businesses or insurers to pay ransom or extortion demands:





Recommendations from AISA for government:

Work with OCSC and accelerate the program to perform CMMs with our neighbours to better understand their level or maturity, understand the gaps that need to be addressed and define / execute projects with our neighbours to close those gaps. Only when our neighbours are assessed, and a plan is developed to uplift areas that might need maturing, can we actually identify and discuss mechanisms to build regional cyber resilience and better respond to cyber incidents as a collective region.

3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

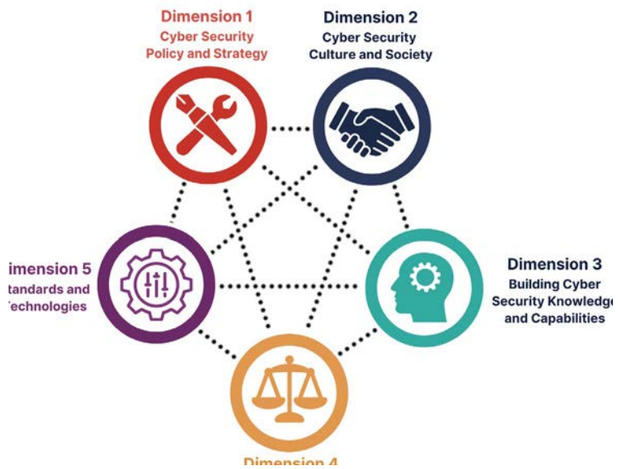
The OCSC is comprised of multiple university members and industry partners with over 120+ specialists in cyber security.The Oceania Cyber Security Centre (OCSC) is perfectly placed to assist Federal Government to coordinate, facilitate and execute projects with our regional neighbours. This Australian talent combined with the OCSC's University of Oxford's Cybers ecurity Capacity Maturity Model for Nations (CMM) work that is being conducted in the region should be amplified and accelerated. The OCSC continues to work with partner nations and the international cyber security capacity building community, on research and capacity building projects that meet the identified needs and requests of partner nations, toward a safer and more secure digital environment for all.

As part of the global constellation of capacity centres working with the University of Oxford's Cybersecurity Capacity Maturity Model for Nations (CMM), at the invitation of governments, the OCSC conducts multi-stakeholder national cyber security capacity assessments. The Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford developed the CMM as a framework to facilitate the review of the maturity of a country's cyber security capacity in consultation with 200+ international experts drawn from governments, international organisations, academia, public and private sectors, and civil society. The CMM continues to be refined through expert consultation, with the latest version released in March 2021. As of December 2021, the CMM has been deployed 120+ times in 87 nations across the globe.

The CMM considers that developing effective national cyber security policy and strategy must include:

- encouraging responsible cyber security culture within society;
- building cyber security knowledge and capabilities for the existing and future workforce;
- creating effective legal and regulatory frameworks; and
- controlling risks through standards and technologies.

Importantly, the CMM takes a view of cyber security that extends beyond IT, to the five dimensions, as pictured in the graphic.



OCSC has performed CMM reviews for: Cook Islands, Tuvalu, Federated States of Micronesia, Vanuatu, Papua New Guinea, Samoa and Tonga.

4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

There are many opportunities, including CMMs in the region and working with OCSC through to training and skills partnerships to build capacity. There are secondment opportunities and trade opportunities for Australian based firms to sell services to countries in the region.

The opportunity for student exchanges from high school to university level studies should be a priority. Students become workers and that kind of understanding of other cultures and perspectives is priceless when it comes to then creating and maintaining bilateral and multilateral partnerships in cyber security (and indeed all facets of government policy) perspective. We note that for example the recent trilateral arrangement between the US, Japan and Australia, there is scope for cooperation that includes technology, cyber security and AI. These three fields interplay. Japanese is a language already taught in many schools around Australia and some exchanges no doubt already exist. Encouraging exchanges as a policy for schools undertaking foreign language studies helps feed a better-informed Australia population. Making this specific to cyber security would involve adapting the school curriculum to expand computing subjects to include an element of cyber security.

The reason that starting early (i.e. prior to tertiary education settings though of course exchanges at the tertiary level are also very beneficial) is that in Australia we have often left it 'too late' for students – and ultimately our adult population – to properly understand computing and cyber security. If you observe the work done by one of our closest allies, the US, they commence coding and cyber education in elementary school and that is continued throughout their curriculum. The US also have in their undergraduate degree programs usually the first 2 semesters dedicated to 'generalist' studies where students pick up skills useful in all workplaces. While that is a separate argument for academic specialists it is possible, we would improve our capacity to elevate our existing partnerships globally by ensuring that across the education spectrum from primary schools to tertiary students are exposed to and taught the 'basic 5' of cyber security. It needs to be inculcated into our culture much as other programs like 'stranger danger' have been in the past. Until we do this we are oftentimes more of a burden for our bilateral and multilateral partners because we rely on their skills and knowledge to supplement our gaps.

We also note that if the government continues to fund the same cyber security silos it will inevitably arrive at the same outcomes, and we recommend diversifying investment more broadly. The same voices have been echoing in the cyber security field within Australia for some time and until we allow space for newer Australians (recently migrated for example) or gender diverse voices to be heard we must expect less innovation. In this vein we recommend considering offering funded exchanges both in and out of government for academic and working cyber specialists to experience for example, three months to a year of working with one of our international partners. This not only works as them being an ambassador for our skill base and culture, but it also means the individual brings back the understanding of the partner country culture. Defence has long had exchange postings with allied nations for this reason. It is a significant long-term investment, and the rewards are reaped over many decades much beyond the term of any one government. We could do more to make our complex array of cyber related, data related, privacy related and security related laws more digestible for foreign partners.

5. How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

Australia is currently working on international standards-setting via Standards Australia Under Standards Australia the working group known as IT-012 with representatives from government and industry work across global standards and the adoption of exiting international standards into Australia.

Over the next 12 months working group IT-012 plans to adopt numerous international ISO and ETSI standards into Australia which will be classed as either Australia, or jointly Australian and New Zealand standards.

Australia contributed to the UN OEWG developments in the field of information and telecommunications in the context of international security in 2021 and this work is ongoing.

To this end the Cyber Law Map (https://austlii.community/wiki/CyberLaw/) was created in 2020 and with a small amount of financial assistance could be kept up to date – it is the only place to find the array of relevant case law and regulation for Australia.

In 2019 the Australasian Cyber Law Institute was formed with the mandate to promote ethics in the intersect of law and cyber. The Institute has the aim to extend from the Australasian region to international because cyber space does not recognise the Westphalian construct of nation state borders. The type of innovation that ACLI represents is frequently available in plain sight, however the failure of the current funding ecosystem to support and promote such work means that Australia is frequently playing catch up, in both its own responsible state behaviour but also in being able to support coalition and other neighbours in upholding responsible state behaviour in cyberspace. To better promote international standards, Australia needs to have its 'own house in order' as regards the current unclear and fractured cyber laws/standards that exist. The simpler our own structure is the better we will be able to enforce laws and standards domestically and have partners assist us to enforce them.

The previous Australian Cyber Security Strategy focused very heavily on defence related cyber projects compared to civil cyber infrastructure. It is important to ensure civilian aspects of laws, norms and standards are not neglected. To that note Australia requires a Cyber Ambassador who is interested and willing to engage globally and regionally to promote the alignment of laws, norms and standards across our closest partners and strategically important regional neighbours.

6. How Government departments & agencies better demonstrate & deliver cyber security best practice?

AISA suggestions by demonstrating following capabilities:

- **Robust policies and procedures:** establish and enforce robust policies and procedures for cyber security, including regular risk assessments, incident response plans, and access controls. These policies and procedures should align with industry best practices and relevant standards. While the Essential 8 might be perfect for Defence systems where costs are not a barrier, the cost to benefit ratio, and practicality of full implementation needs to be considered in line with the risk appetite of other government departments.

- **Advanced controls:** implement advanced technical and process controls to protect IT systems, networks, and datasets. Regular security testing and vulnerability assessments should also be conducted to identify and address potential weaknesses in systems and operational processes.

- **Skilled and trained workforce:** invest in developing a skilled and trained workforce to handle cyber security challenges effectively. Design regular cyber security training and awareness programs for employees at all levels. Additionally, hiring and retaining skilled cyber security professionals to implement and maintain effective cyber security measures.

- **Collaboration and information sharing:** foster a culture of collaboration and information sharing within their departments and with other entities. Share threat intelligence, best practices, and lessons learned from cyber security incidents to enhance the overall cyber security posture of the sector. Collaboration should also extend to industry, academia, and other stakeholders, and to share expertise and resources jointly when addressing cyber security challenges.

- **Compliance and accountability:** comply with relevant laws, regulations, and policies related to cyber security, and hold employees and contractors accountable for their actions. This includes monitoring and auditing cyber security practices to ensure compliance, as well as taking appropriate disciplinary or legal action against those who violate established policies or procedures.

- **Continuous improvement:** strive for continuous improvement in their cyber security posture. This includes regularly reviewing and updating policies, procedures, and technical controls to adapt to evolving threats and changing technologies. Conducting post-incident reviews and implementing recommendations for improvement can help enhance cyber security practices and serve as a model for other entities.

- **Australian Public Service** should less rely on consultancy firms when it comes to implementation, and look at opportunities to better use industry expertise to assist with projects etc. Engaging industry to provide oversight will enable APS with better cost to benefit management and to identify project/ engagement outcomes that no longer align with the objectives of the initiative.

By implementing and demonstrating strong cyber security practices, Government departments and agencies can serve as a model for other entities, including private sector organisations, non-for-profit organisations, and individuals, and contribute to the improvement of cyber security across the sector.

7. What can government do to improve information sharing with industry on cyber threats?

The government should foster a culture of collaboration and information sharing between government agencies, industry, academia, and other stakeholders in the context of cyber security. At the roundtables and townhall sessions, common feedback was that the government needs to be less "secretive" and operate less like an "intelligence agency" and instead be more helpful. The sector asks for a more transparent role from the government and expects it to produce tools and insights that can help businesses in real time - especially in instances of scaled cyber-attacks OR significant zero days. Establishing a consortium or platform for open and free information sharing can greatly contribute to improving cyber security practices and mitigating cyber threats.

It is crucial for the government and agencies such as the Australian Cyber Security Centre (ACSC) to play a proactive role in assimilating national and business cyber risks. This includes correlating isolated cyber-crimes with nation-state or state-sponsored activities, as cyber threats can often have national security implications. Sharing relevant information, intelligence, and insights about cyber threats and attacks can help all stakeholders, including government agencies and businesses, to better understand the landscape, assess risks, and take appropriate measures to protect against cyber threats, while solving challenges jointly.

91.3% of the sector are in favour of leveraging incidents reported through the Notifiable Data Breaches (NDB) scheme to build case studies and education materials to educate the public, businesses and directors on real world incidents. Only 3.2% were not in favour.

To encourage information sharing, it is important for the government to provide assurance that the information shared will be used solely for the intended purpose and will not be misused or shared with other government agencies or regulatory bodies without consent. Ensuring confidentiality and protection of sensitive information can help build trust and encourage greater participation in information sharing initiatives.

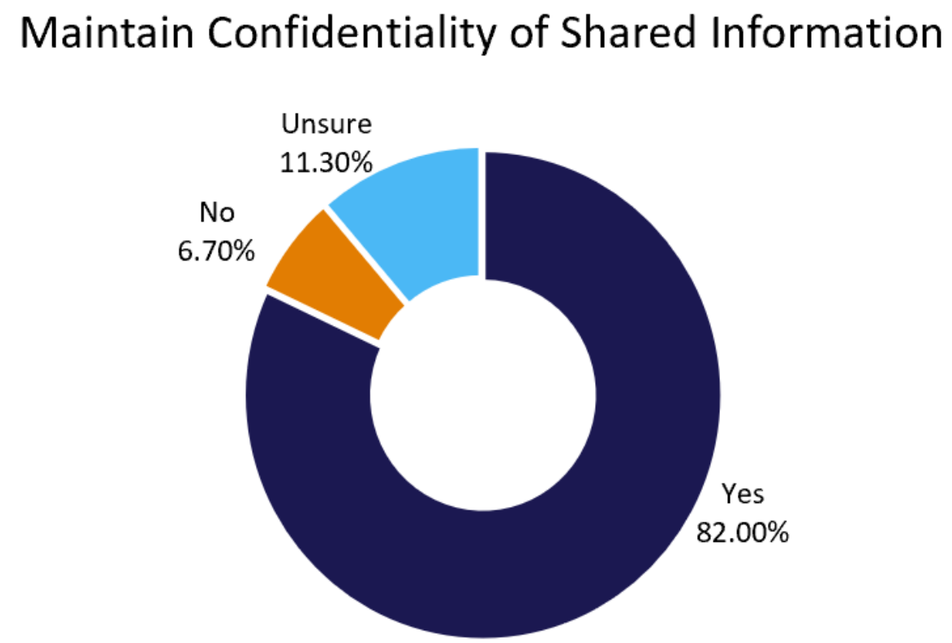
The government should also re-introduce the state information-exchanges that are currently held in the JCSCs, and also work on regional area (e.g. Bendigo, orange, Townsville). Awareness sessions and regulator meet ups should also be organised outside of the JCSCs for SMEs, and these should be then jointly held with COSBOA.

It is also essential to discourage victimisation of any entity or individual that falls victim to a cyber-crime. Cyber security incidents can happen to any organisation, and it is important to approach incidents with a collaborative mindset, focusing on mitigation, remediation, and prevention rather than blame or finger-pointing. Creating a supportive environment where organistions feel comfortable reporting cyber incidents without fear of repercussion can foster a more effective collective response to cyber threats.

8. During a cyber incident, would an explicit obligation of confidentiality upon the ASD and ACSC improve engagement with organisations?

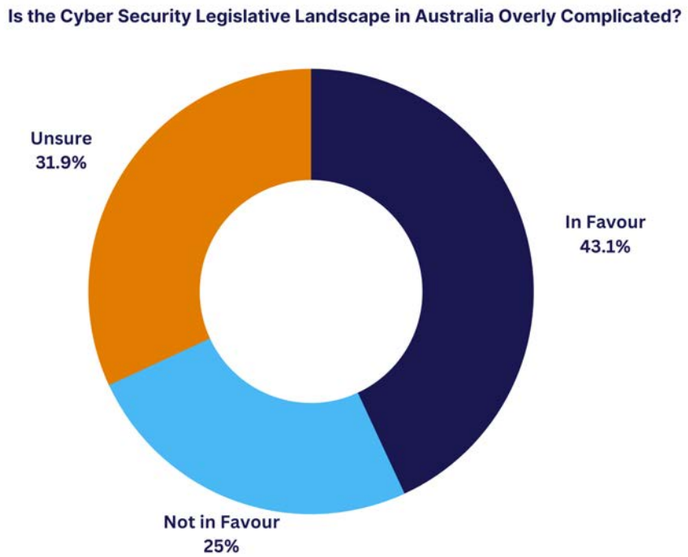
To encourage information sharing, it is important for the government to provide assurance that the information shared will be used solely for the intended purpose and will not be misused or shared with other government agencies or regulatory bodies without consent. Ensuring confidentiality and protection of sensitive information can help build trust and encourage greater participation in information sharing initiatives. This information sharing should also be protected against Freedom of Information requests, and similarly the shared information should not be allowed to be used against organisations in civil actions.

There is strong evidence from respondents where 82.0% of the cyber security industry and senior leaders are in favour of maintaining confidentiality when sharing information with ACSC and ASD. This significant support indicates intentions within the sector to be more collaborative on matters dealing with cyber security, but for it to be contained and privacy and confidentiality to be maintained against any other use by government and any agencies. 6.7% are not in favour and 11.3% of respondents are unsure.



9. Would expanding the existing regime for notification of cyber security incidents improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime?

At the roundtables and during townhall sessions, the general consensus within the sector is the concern about the potential burden of additional mandatory reporting requirements on organisations that are already grappling with regulatory compliance challenges. It is important to balance the need for better understanding of the quantum of the problem, related to ransomware incidents, with the potential burden on organisations is important.

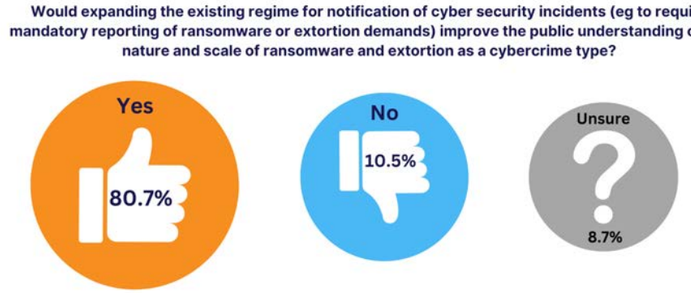


43.1% believe the cyber security legislative landscape in Australia is overly complicated. 31.9% are unsure.

Creating a culture of collaboration and information sharing, as described in our recommendations to questions 7 & 8, can be an effective approach to address this issue. By fostering an environment where organisations feel safe to come forward and share information openly, seek help, and collaborate on combating cyber-crimes like ransomware, organisations can benefit from collective insights and expertise without feeling overwhelmed by regulatory compliance.

However, when AISA asked the broader cyber security community if expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) would improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type 80.7% responded “Yes”, 10.5% responded “No” and 8.7% were unsure.

This significant support indicates intentions within the sector to be more collaborative on matters dealing with ransomware, but for the purposes of better understanding the risks and challenges that are associated with cyber-crimes such as ransomware and not for use by government or any other agencies.



Based on the feedback from the sector AISA recommends establishing a safe harbor for organisations to share information and encourage more affected organisations to participate and contribute to the collective understanding of the threat landscape, without fear of repercussion or possibility of any regulatory penalties or during any civil proceedings. This can help in generating a more comprehensive and accurate picture of the magnitude and nature of ransomware incidents, and enable stakeholders to develop effective response plans, strategies, and solutions.

This could also help in bridging the gap in available data on ransomware incidents and facilitate a more informed and coordinated response to combat cyber-crimes, without the unnecessary apprehension about fronting any regulatory consequences when reporting ransomware incidents.

10. What best practice models are available for automated threat-blocking at scale?

AISA recommends that this is done using a three staged approach:

Collect - Threat intelligence sharing between nations, within the government agencies and the industry is the first step towards sharing the information on new and changing threats around the world. Threat intelligence sharing can also facilitate the development of more robust cybersecurity strategies and defences by leveraging collective knowledge and expertise. This can help identify potential threats early, allow for timely threat mitigation measures, and enable a more coordinated response to cyber incidents. At this stage this does happen between governments at the CERT level and within the five-eyes nations, however, this should be cascaded to the industries regionally. Similarly, industry should be encouraged and incentivised for participating in such a consortium to share information.

Validate - This should then be validated by a conglomerate of cyber experts from the government agencies, industry, academia, and other stakeholders, to confirm the threats and triage based on severity. Having a diverse group of experts with different perspectives and expertise can provide a more comprehensive analysis of threat intelligence, including its severity and potential impact. This can help prioritise and triage threats based on their severity, urgency, and potential consequences, allowing organisations to allocate resources effectively and respond in a timely and appropriate manner.

Distribute and Block – This information should then be distributed to all organisations in almost real-time. This information should include detailed information about the threats, their characteristics, and any patterns that have been observed. This allows organisations to analyse the threat intelligence and compare it with their own observations and experiences to identify potential patterns or trends. Under the current Cyber Threat Intelligence Sharing (CTIS) Program, organisations feel limited due to the legal requirements CTIS is directed to operate under, making it hard to be operational and effective.

The above approach should be underpinned by use of the technologies that are currently available, such as:

Monitoring and scanning of deep and dark web traffic, machine learning and AI for pattern scanning and threat hunting and behaviours analysis models.

11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

Recommendations from AISA:

- All cyber security tertiary courses should be reviewed by a comprehensive expert panel of CISO / CIOs from across several sectors. Courses should be ranked / rated based on relevance and student outcomes for meaningful employment in Cyber Security. The course rankings should be published on a website to enable consumers to select the most appropriate course. Each course ranked / rated should indicate the career pathway that the course is best suited for, to enable consumers to select courses. This competitive ranking would drive better competition between Tertiary providers to ensure their courses are relevant and best suited to the selected career pathways. It also provides consumers with greater transparency and a way to compare courses.

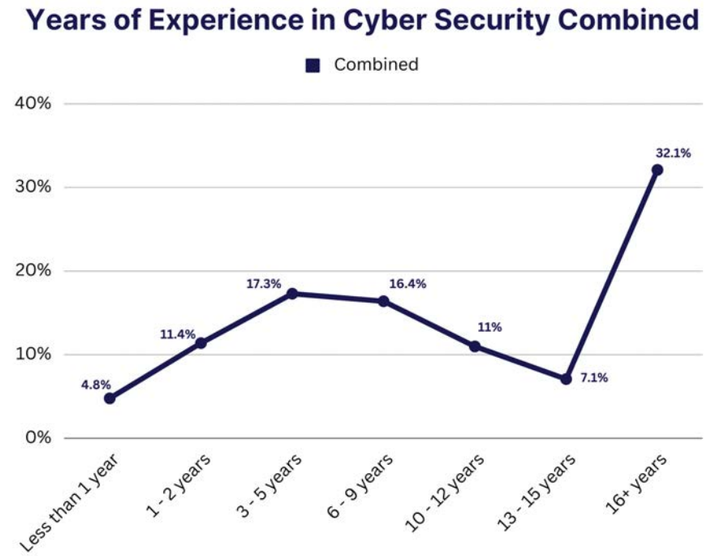
- Tertiary education providers should actively tap into industry CISO / CIOs to uplift their courses and draw on extensive talent in the sector to teach various subjects. There are a lot of cyber security experts with over 20 years of experience who are looking for ways to give back to the community and sector and this could be one mechanism which is formally recognised through Industry or Adjunct professorships.

- Teachers in tertiary education should be provided with industry secondment opportunities to gain real world experience in industry, government departments or both.

- While the adoption of vendor neutral Industry Certifications can lead to artificial and de facto benchmarks which may or may not be suitable, the experience gained from educators obtaining certifications such as CISM, CISSP or equivalent dramatically increases the diverse knowledge and reputation of those educators.

12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

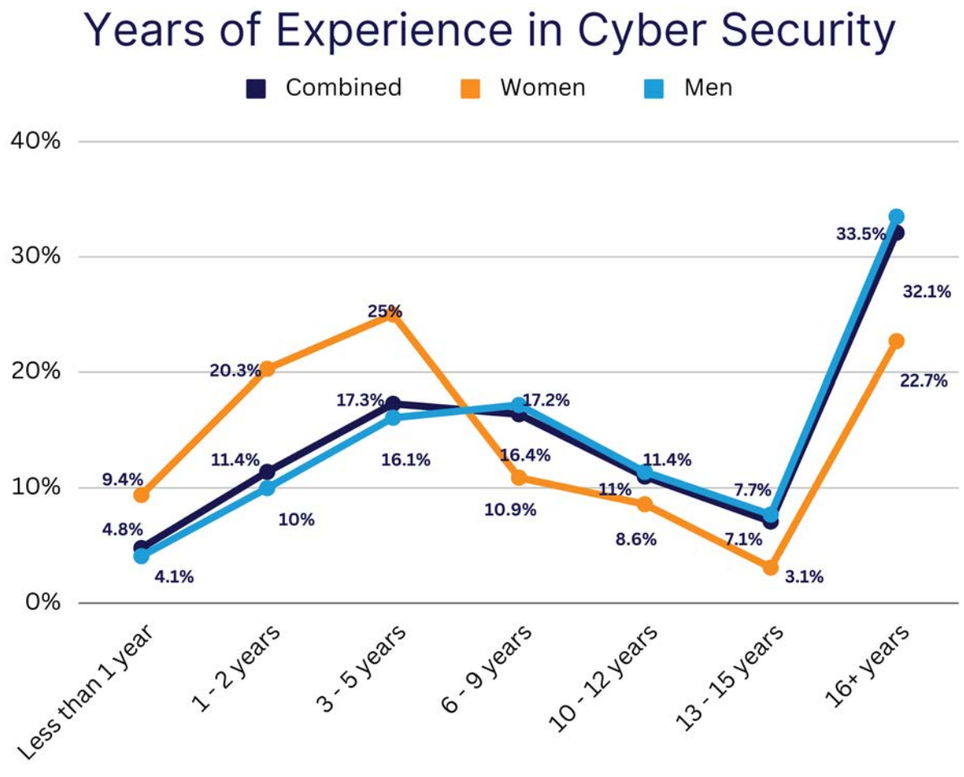
AISA conducted research to determine the number of years cyber security professionals have been in the sector. Almost one third of cyber security professionals working in the sector have greater than 16 years of experience while only 4.8% of professionals have less than one year of experience. Based on the data, we are not seeing people entering the sector within the last two years in the volume needed to sustain the talent pool for future years. Consequently, we can expect to see a deficit of talent in the market for the foreseeable future. This is likely to be exacerbated if professionalisation is introduced, suggesting professionalisation should be put on hold until volumes and diversity increases. Of concern is understanding why the sector experienced a slump in attracting talent between nine to fifteen years ago. With almost 1 in 3 cyber security professionals having more than 16 years of experience the sector demonstrates a high degree of skills maturity, but also fragility over the next 7 to 10 years as some of those individuals retire, move into leadership roles or leave the sector to follow second careers.



When we examine years of experience in cyber security with a gender diversity lens we do see an increase in women entering the sector, compared to men, however post 5+ years of experience there is a rapid decline which suggest several aspects: Futher analysis is required to also identify what campaigns or messaging was used 3 -5 years ago that may have led to an increase in women joining the sector.

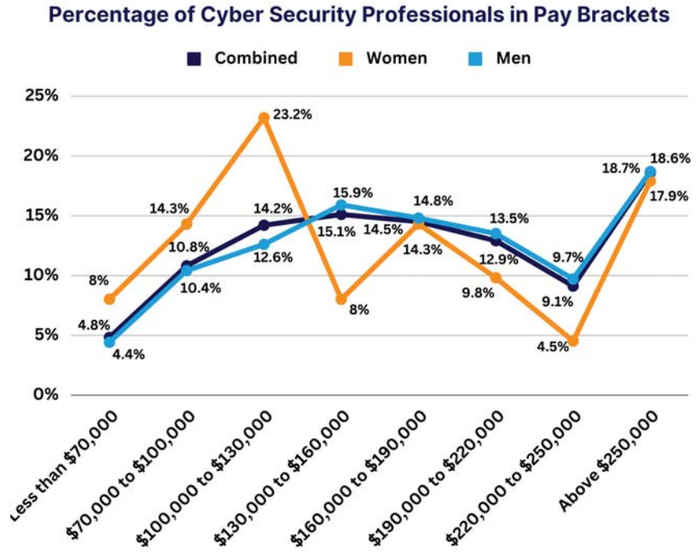
- As a sector we need to make a conscious effort to ensure life changes such as having a family does not deter women from continuing a career in cyber security.

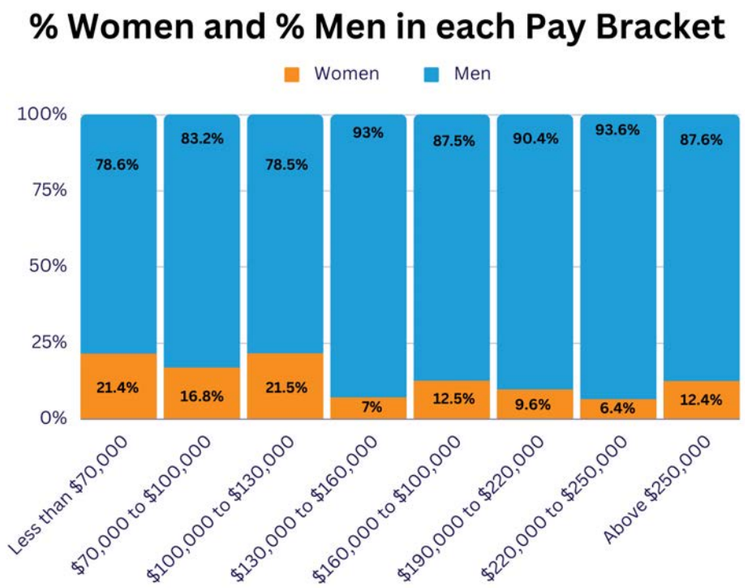
- Anecdotal evidence indicates some women experience adverse working conditions in a male dominated sector which does take a toll on the mental resilience of some women. This is often evidenced in the workplace where a male can make a suggestion about a change they disagree with and it is taken on notice or considered. Whereas a woman can make the same suggestion in the same circumstance and the view is they are being emotional rather than rational. This disparity in perception suggests greater support networks are required for women, especial in leadership roles to retain talented women in those roles.



AISA performed a review of pay brackets in the sector and found that 18.6% of cyber security professionals earn over $250,000 per year, with 43% earning between $100,000 and $190,000. It was surprising that more individuals earn greater than $250,000 a year compared to the pay band of $220,000 to $250,000 by almost 9.5% and that less cyber security professionals are in this pay bracket.

When we break the data down by gender, a different story emerges, highlighting the disparity between men and women when it comes to pay in the sector. While the top earning individuals seems to only have a gender gap of around 0.8%, the gender gap become much more apparent with less women earning in the $220,000 to $250,000 pay range with a difference of 5.2% compared to men, and $130,000 to $160,000 pay range with a difference of 7.9%. More women are in the $100,000 to $130,000 pay bracket with a difference of 10.6% compared to men and disproportionately more women earn at or below the $70,000 to $100,000 pay bracket than men. While the gender diversity challenge still exists within the cyber security sector, the pay gap differences with more women in lower paid roles does not help increase the participation rate of women. Over the last six years the number of women has increased from the lows of 12% to 17% participation in 2023, however 17% is still shockingly low and more work needs to be done in primary and secondary education to attract more women to the sector.





More than $250,000 salary bracket

There is a strong correlation in the data that people with over 16 years of experience in cyber security are paid above $250,000. There are some exceptions with people with limited experience still earning over $250,000, however these job roles tend to be Sales or Account Management focused. Sales and Account Management jobs typically can have an OTE (On Target Earning) capacity of over $250,000 per year, however OTEs can have 20% to 50% of the salary at risk if these individuals fail to meet their sales quotas. This essentially means the base salary could be in the range of $120,000 to $150,000 and only reaches over $250,000 as sales or quotas are met within a 12-month period.

Typically job roles earning over $250,000 per year with greater than 6+ years experience that are not sales based are: Chief Security Officer (CSO), Chief Information Security Officer (CISO), Chief Technology Officer (CTO), Director of Cyber Security, General Manager, Head of Cyber Security, Security Architect, Senior Security Specialist and Principle or Senior Consultant.

$220,000 to $250,000 salary bracket

Job roles earning between $220,000 to $250,000 per year are the same as those in the $250,000 pay bracket, but with the inclusion of some Risk Management and Cyber Advisory roles.

The gap between the number of cyber security professionals in this pay range appears to be increasing between Victoria and New South Wales. In the above $250,000 pay range, the gap is only 7.9%, in the $220,000 to $250,000 range it increased to 11.5% more professionals in Victoria compared with New South Wales. In the next pay band ($190,000 to $220,000) the gap is 10.9%.

$190,000 to $220,000 salary bracket

When reviewing the $190,000 to $220,000 salary bracket it was noted job roles typically are: Cyber Operations Manager, Senior Security Engineer, Cyber Security Educators, Security Architects, Consultants, Program Managers, Heads of Cyber Security with the occasional Chief Information Security Officer from government sectors.

Almost one in four people with 16+ more years of experience are in the $190,000 to $220,000 pay bracket. One third of this segment have between 3 to 12 years of experience.

Western Australia more than doubled the number of cyber security individuals in this pay band compared to the previous pay band and the ACT has more than halved in the number of people. Queensland has had significant growth from 3% to 15.2% in this pay band compared to the other states.

$160,000 to $190,000 salary bracket

The number of cyber security professionals in the $160,000 to $190,000 pay band continues to increase for those with between 3 to 10 years of experience. Those with 16+ years of experience are still seen in this pay band, however in declining percentages.

The types of cyber security roles in this pay band include: Cyber Security Product Managers, Researchers, Delivery / Project leads, Consultants, Advisors, Auditors, Managers, Government CISOs and Directors.

$130,000 to $160,000 salary bracket

In this pay band we see a larger reduction in cyber security people with 16+ years of experience and a larger influence of those with 3 to 5 years and 6 to 9 years experience. Job roles in this bracket include: More academics and researchers, GRC analysts, Service Delivery Managers, Security Analysts, Cyber Risk Managers, Consultants, Cyber Assurance Auditors, Incident Responders, Engineers and interestingly some more junior Cyber Security Architect. This aspect is interesting as Cyber Security Architects are much more predominantly seen in higher pay bands due to the demands for their skills.

Tasmania seems to have more cyber security professionals in the $130,000 to $160,000 pay band than the previous band of $160,000 to $190,000. Victoria has dropped in the number of professionals in this pay band and so has NSW with growth going mainly to South Australia

$100,000 to $130,000 salary bracket

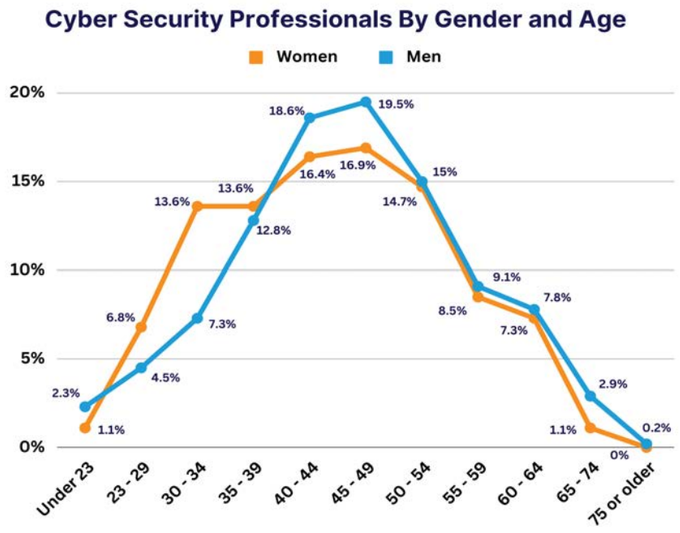
In this pay bracket the dominating group of cyber professionals typically have between 1 to 5 years of cyber security experience.

Queensland, South Australia and Western Australia have moved ahead, pushing New South Wales into 5th place for individuals with this level of pay. This could be down to the cost-of-living pressures in New South Wales or a combination of other factors. Victoria for example continues to have the Certificate IV in Cyber Security offered free at TAFE. Queensland introduced it free in 2022 and South Australia / Western Australia are offering it free in 2023 at TAFE.

$70,000 to $100,000 salary bracket

In this pay bracket the dominating group of cyber professionals typically have between 1 to 5 years of cyber security experience, similar to the $100,000 to $130,000 pay bracket. As expected we only see a smaller number of highly experienced individuals in this pay bracket. What is interesting is we would have expected more people with less than 1 year due to the large volumes of students completing degrees or certificates in cyber security. However there is strong evidence many students are unable to find jobs in cyber security as they lack hands on work experience.

New South Wales has move up from fifth spot, to fourth in the state rankings with Victoria in a strong dominating lead (41.2%) which is likely to be due to the free TAFE Certificate IV playing a large part.



Support for professionalisation of the sector continues to be mixed with the biggest proponents of professionalisation in the academic sector. 72.6% of academics feel a professionalisation scheme should be introduced into Australia, while interestingly only 39.5% of those who employ cyber security professionals actually support a professionalisation scheme. 42.5% of Executives and CISO/ CSOs do not support a professionalisation scheme. If professionalisation is not supported by industry Executives and CISO / CSOs, it will fail to be adopted by cyber professionals. It also raises the question, what problem is professionalisation trying to solve, especially if it is not supported widely by industry? In both technical and non-technical cyber security professions, support for professionalisation of the sector hovers around 50%. When gender is considered, there is less support from women for professionalisation. An alternative approach which has widespread support across the cyber security sector is the licensing of cyber security Managed Service Providers (MSPs). This type of licensing scheme would negate challenges seen in other programs such as the Pink Batts Insulation scheme, where unregulated operators caused issues for the whole sector. In a model where the operators or providers hold the license or accreditation to provide trusted cyber security services, accreditation moves from the individual to the provider of the service. This licensing or accreditation model is supported by 74.7% of the sector with only 14.4% not in support and 10.9% unsure.

Based on gender and age analysis, focusing exclusively on women and men at this stage (not including individuals who do not dentify as either), one in three cyber security professionals are aged between 40 and 49. Over 65% of cyber security professionals fall within the 35 to 54 years age bracket. It is concerning that there is not a higher proportion of individuals aged 23 to 34 to replace those in the above 50 years age range, who constitute one-third of cyber security professionals and may be contemplating leaving the sector, reducing their work hours, retiring, or pursuing a career change. Cyber security professionals who prefer to self-describe their gender account for 0.5% of the workforce.

Recommendations from AISA:

- Workforce issues relating to skill shortages in the supply and demand side are complex and cannot be resolved by using professionalisation or accreditation. It should be noted that professionalisation or accreditation will only disadvantage more women and drive them away from the sector.1
- More focus and attention is required to rapidly boost the number of girls in primary and secondary school who want to have a career in cyber security, in order to boost the number of women participating in the sector. In addition, more women can transition into the sector from non-traditional entry pathways into cyber security. Great areas to draw on, which will become increasingly more important in the future due to the skills they bring to the sector will be the areas of psychology, sociology, humanities and risk management. Some of these areas naturally have a higher proportion of female participation which should be encouraged to transition to cyber security, especially as the focus moves away from just being a technology problem and more balanced to include the human, societal and business risk problem spaces.

13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

impact and severity of the incident. As we witnessed during the recent data breach incidents, the information shared from the government and these organisations at times were in conflict or uncovered details that were not coherent. Consistency in messaging, both internally and externally, is important to avoid confusion and maintain public trust.

Support for affected entities, including businesses and individuals, should be a priority. The government should provide assistance and resources to help them recover from the incident, which may include financial support (for SMEs), technical expertise, and guidance on response planning.

Public-private collaboration is critical in addressing cyber threats. Strengthening partnerships between the government and the private sector, including critical infrastructure operators, can enhance cyber defences and response capabilities. This may involve regular engagement, information sharing, joint exercises, and collaborative efforts to identify and address cyber threats proactively.

Overall, effective collaboration, communication, and coordination among the government, response agencies, affected entities, and the private sector are key to effectively responding to major cyber incidents, mitigating their impact, and improving cyber security resilience at a national level.

a) Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

Many organisations find current regulatory and mandatory reporting requirements complex and overwhelming. Cyber security compliance can be challenging, especially for organisations whose primary business function is not related to technology, and it can be seen as an added risk rather than a core function.

To address this, the government can focus on providing clear and concise guidance on regulatory requirements, avoiding duplication of efforts, and minimising unnecessary complexity. This can help organisations better understand their obligations and implement appropriate measures to comply with regulations without undue burden.

There is strong evidence in the survey where **91.1% of the cyber security industry and senior leaders are in favour** of harmonising existing requirements to report separately to multiple regulators and believe that it will be beneficial to have a single reporting portal. This significant support indicates that organisations understand the importance of reporting to regulators and other agencies but find it complex and overwhelming. AISA recommends that an omnichannel portal should be designed where reporting is seamless and effortless, allowing for effective mandatory reporting which is then cascaded within and between various government agencies and regulatory bodies. Only **2.9% are not in favour with 6.0% being unsure.**

Overall, balancing regulatory requirements with the operational realities and resource constraints within the sector, and providing support and guidance, can help organisations better comply with cyber security regulations without feeling overwhelmed.

14. What would an effective post-incident review and consequence management model with industry involve?

For all major cyber security incidents and data breaches it should be mandatory to conduct a post-incident review. The post-incident review should be comprehensive and should clearly articulate the causes and events leading up to the major incident. The post-incident review process should be thorough, involving relevant stakeholders from both technical and business functions to uncover any systemic issues that could be responsible for leading towards the major security breach. Mandatory post-incident reviews, particularly for publicly listed organisations, can help ensure transparency and accountability, and provide valuable insights for continuous improvement in cyber security practices.

Subsequently, incorporating the findings and recommendations from post-incident reviews into the organisation's existing risk management profile is an important step. It allows organisations to assess if there were any omissions or unidentified risks that contributed to the cyber security incident or data breach, and if the existing risk assessment and mitigation measures were adequate and aligned with the organisation's risk appetite. The post-incident review can provide insights into any gaps or weaknesses in the risk management approach, including the accuracy of risk ratings, effectiveness of mitigating controls, and overall risk posture. The findings and recommendations from the post-incident review should be incorporated into the ongoing risk management practices, which reinforces the importance of aligning cyber security with overall business risk management objectives.

The review should emphasise the need for actionable and prioritised corrective actions to address the lessons learned from the incident and strengthen the protection of systems and data to avoid future incidents. The review should also highlight the importance of evaluating the findings and recommendations as part of the overall risk management process. This will ensure that the organisation's risk profile is not overlooked, and that proactive measures are taken to prevent falling back into a complacent "cruise-control" mode.

The industry should take the lead in designing a comprehensive consequence management model leveraging its expertise and experience, rather than relying solely on government and other agencies for regulatory requirements. However, the government should consider implementing a mandatory reporting requirement for post-incident reviews of significant breaches for all public and private entities. This would ensure that organisations conduct thorough reviews and learn from incidents, while also providing valuable insights for regulatory oversight and industry-wide improvements in cyber security practices.

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

Improving cyber security best practices and supporting victims of cybercrime requires a collaborative effort between government, industry and the wider community. Industry in this context refers to the broader economy encompassing commercial enterprises (for example, solution providers, Managed Service Providers (MSPs), Small to Medium Enterprises (SMEs), large Enterprises both public and private and vendors), not-for-profits, education providers and peak industry bodies like AISA.

While establishing a national cyber security strategy is only the first step, it is a critical aspect. The government should work with a broad cross section of industry partners to develop a comprehensive and up-to-date national cyber security strategy which clearly outlines clear objectives and priorities for enhancing cyber security across public and private sectors, has measurable goals and will deliver frequent and honest reporting on progress for transparency. Individuals involved should be experts not only in cyber security, but government policy, challenges faced by businesses small and large, the education sector and have deep understanding of social sciences. The current government has failed to deliver such a body to oversee the creation of the new 2023-2030 cyber security strategy.

Recommendations from AISA:

Expert Advisory Board to include individuals from: individuals from:

- industry and government departments (State and Federal) with hands on experience of dealing with the challenges of keeping their organisations safe on a day-to-day basis and to gain a better understanding of the demand side skills challenges.
- small business representation to truly understand awareness of the risks, the daily challenges, and priorities of this segment.
- education sector representation to address the supply side challenges to skills.
- sector representatives such as AISA and TCA (Tech Council Australia).

- Promote public-private partnerships where government contributions either through funding or resources can be amplified to deliver greater positive impacts across a whole sector or multiple sectors. Collaboration between government agencies, industry partners, and academic institutions to share information, resources, and expertise to improve cyber security practices and develop new technologies should be encouraged and assessed from a positive productivity perspective. For example, every dollar invested by government should generate greater returns either through harm reduction, cost reductions, productivity increases and safety improvements.

- Strengthen cyber security education and training with a focus on delivering on measurable outcomes that delivers an improved skilled workforce, increases student employability, and provides increased access for industry (small and large enterprises) to access talent on a national level, including remote talent in regional and rural areas.

- Improve cyber security incident reporting and support mechanisms by implementing a single front door with dedicated channels for reporting cybercrime incidents and coordination with the various agencies and regulators. Provide support services for victims, including access to legal and financial assistance, counselling, and advice on how to prevent further attacks. This type of service should be available for Australian citizens and Australian businesses.

- Encourage information and experience sharing by promoting a culture of information sharing and cooperation between businesses, government agencies, and other stakeholders to help identify and mitigate potential cyber threats, but more importantly the lessons learned to improve resilience and reduce the occurrence or harm of similar incidents in the future. Communication from government needs to be tailored to the segment. While the ACSC has fantastic resources on the website, it has completely failed to speak the language of small businesses and the not-for-profit sector.

- Launch campaigns to raise public awareness with both individuals and businesses for cyber security risks, prevention measures, and responding to cybercrime incidents. The use of case studies above could feed into the campaigns and act as guides. The objective is to raise awareness, drive long lasting behavioural change and education. A similar approach to the very effective “Slip Slop Slap” campaign which drove a greater understanding of skin cancer among the general public and provided them with a simple mechanism to reduce the occurrence, hence harm reduction.

a) What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

A holistic approach is required to address the complex challenge of helping small business. Small business needs:

1. Help understanding they are at risk (e.g. the who, the why and the what will be most likely targeted).
2. Simple relevant guides that illustrate how they could be harmed.
3. Introductions to support networks so they can discuss with peers to ensure they do not feel alone. Enable them to share solutions and ideas to reduce the harm to their businesses.
4. Notifications either via local newsletters, similar to Neighbourhood Watch programs that report on crime trends, issues in the local area with helpful tips that resonate with their needs and support numbers to call for further information.
5. Technology vendors or the opensource community to build tools small businesses can use that are easy to use, low cost to own and maintain.
6. Legislation that forces Technology vendors to provide solutions in Australia that are secure by default and the business owner can make a choice if they want to reduce that level of security (e.g. automatic updates, no default passwords, unnecessary services turned off, integration into password management systems etc).

Items 1 to 4 could be delivered via local community groups, local government initiatives, AISA, COSBOA or organisations who these small businesses are either customers or part of their supply chain. For example, PEXA, the online Property Settlement, Tracking & Insights provider has access to over 10,000 conveyancers and practitioners who run small businesses. CPA Australia has thousands of members who run small businesses and advise small business owners. NAB and CBA's business banking side reaches out to and communicates with small business daily. These types of organisations should be supported and coordinated by government to help ensure small business owners are being educate and appropriately advised.

AISA runs one of the most comprehensive cyber security conferences in the southern hemisphere called the Australian Cyber Conference. The event runs over three days, has global keynote speakers who talk on topics of leadership, innovation, opportunities and motivation in addition to the other 400+ speakers across 25 concurrent program streams. Not only does the event serve to connect the cyber security community, but it also runs program streams focused on research and uplift of cyber security for small business owners, NFPs, government departments and the general community in Australia. The federal government should officially support the outreach and charitable activities conducted by AISA to work with PEXA, CPA, NAB, CBA and similar organisations to ensure their customers can attend the event to share knowledge, engage in peer conversations and learn how to adopt harm reduction strategies to build safer and more resilient businesses.

16. What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

The Australian government both at federal and state levels could play a crucial part in enhancing the cyber security technologies ecosystem and promote the uptake of services and products nationally and internationally.

Improve collaboration with industry, academia, and sector representatives such as AISA to better understand the needs and gaps within the sector. Establish collaborative cohorts and identify areas and topics to facilitate research, development, and innovation opportunities. The government should consider investment options to foster innovation which include tax incentives for organisations or grants for sector representatives to help with development of sovereign cyber capabilities.

89.3% of the cyber security sector is in favour of establishing more apprenticeship programs which enable direct placements within Australian companies. Similarly, **82.8% of the sector supports tax benefits to be granted for organisations which assist with on job upskilling programs.** The government can support organisations through tax subsidies to run more internship programs, solving the challenges with workforce while establishing more sovereign capacity for Australian services and technologies.

Another opportunity that the government could drive is through procurement and adoption within the government agencies and critical infrastructure operations for Australian cyber security services and products. We could take inspiration from the 'Make in India' concept that was initiated in India 8 years ago to create and encourage companies to develop, manufacture and assemble products made in India and incentivise dedicated investments into manufacturing. This could create a market demand for cyber security technologies and the government incentivises local organisations to develop and offer innovative solutions. **81.4% of the cyber security sector favours any initiative taken by the Australian government to better use procurement as a lever to support and encourage pathways to market Australian owned cyber security services and technologies.**

The government could also assist already established Australian companies to expand into overseas markets by creating improved export promotions and facilitating international market access through agencies such as DFAT. Similarly, improved investment opportunities should be explored for overseas investors and venture capitalists by curating investment campaigns and trade missions to global markets and locally. This will help local companies showcase their capabilities, establish partnerships with international counterparts, and explore export opportunities – further enhancing the Australian cyber security technology ecosystem.

AISA is currently exploring partnership arrangements with Plug and Play, based out of the Silicon Valley, and is the world's largest innovation platform and startup accelerator with a global footprint in 20+ countries. AISA would be interested to explore trade and investment KPIs for DFAT and how AISA could assist with building more global presence for Australian companies by leveraging their relationship with Plug and Play.

By doing all or some of the activities recommended above the government could assist with creating a conducive environment for innovation, adoption and foster a thriving cyber security ecosystem sovereignly.

17. How should we approach future proofing for cyber security technologies out to 2030?

- **Maturity assessment** - conducting a maturity assessment is a crucial step in understanding the current state of cyber resiliency at a national level. It will help the government to assess the cybersecurity posture, identify strengths and weaknesses, and determine areas that require improvement. A maturity assessment can provide a realistic baseline to develop a roadmap and set milestones for enhancing cyber resiliency. It also enables to pivot quickly and revise strategies in response to changing threat landscapes or evolving technology trends. By conducting a maturity assessment, government could gain valuable insights and accordingly prioritise investments, allocate resources, and make informed decisions to strengthen cybersecurity defences at a national level.

- **Define the Vision** – A well-defined cybersecurity vision provides a clear direction and sets the stage for developing comprehensive strategies, policies, and initiatives to achieve the desired state of being the most cyber secure nation. It also helps to monitor progress, evaluate the effectiveness of cybersecurity efforts, and adjust as needed to stay on track towards the vision.

- **Gap analysis** – Defining clear and measurable goals is a crucial step in the journey towards achieving the vision of becoming the most cyber secure nation. These goals should be aligned with the overall vision and should be specific, measurable, achievable, relevant, and time bound. They should be based on a thorough understanding of the current state of cybersecurity maturity and the identified gaps and challenges.

- **Who is doing what –** Identifying clear responsibilities and roles for different stakeholders, including the government and the industry, is crucial for effective cybersecurity strategy implementation. While the government plays a vital role in providing overall leadership, coordination, and policy framework, the industry also has a critical role to play in contributing its expertise and capabilities towards achieving the strategic goals. Collaboration and cooperation between the government and the industry are essential to address capability and capacity gaps and ensure a holistic approach to cyber security. The strengths and expertise of different entities should be identified and leveraged to maximize effectiveness. This may include identifying areas where the industry has specialized knowledge and capabilities and allocating responsibilities accordingly. The government can provide assistance and resources to the industry to support its efforts in delivering on strategic goals. This can include tax incentives, financial support, access to information, global relations, and collaboration with agencies such as the ACSC or ASD. Such support can help the industry to enhance its cybersecurity capabilities, invest in research and development, and adopt best practices.

- **Uplift Cyber skills –** As per recommendations stated in response to question 11 above, significant steps should be taken to uplift cyber skills across the board. Regular review of existing cyber courses and programs, both at educational institutions and industry certifications, should be conducted to ensure they are up-to-date and aligned with the changing needs and evolving threats in the cybersecurity sector. Increased funding and resources should be allocated towards cyber education and training programs to promote the development of skilled cyber professionals. Educators who are responsible for delivering cyber education and training should also receive adequate support in terms of professional development and training. Collaborative efforts between academia and industry can help bridge the gap between theoretical knowledge and practical skills. And significant efforts should be made to promote inclusivity and diversity in the workforce.

- **Awareness** - Raise public awareness through comprehensive public campaigns on cyber security risks, prevention measures, and how to respond to cybercrime incidents, targeting both individuals and businesses. It is important to remember that the objective is not to just raise awareness but drive long lasting behavioural change and education.

- **Rinse and Repeat –** lastly, and more importantly – Cyber resiliency is an ongoing process that requires consistent effort and practice, much like training muscles. The government, organisations and individuals need to continuously assess, improve, and adapt their cyber security measures to keep up with the ever-evolving threat landscape.

The above approach will assist in uplifting the overall consciousness about cyber security and will prepare a community of cyber aware individuals. This will drive a fundamental shift towards long lasting behavioural change assisting with better skilled and cyber conscious individuals in the workforce. Better aware consumers and more conscious technologists will future proof technologies for improved cyber resilience

18. Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

There are several opportunities that would greatly support wholly owned Australian cyber security firms. The Australian government could better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure a viable path to market for local firms. Opportunities the government should consider include:

- **Implement a 'Buy Australian First' policy for cyber security products and services within Government:** This would encourage government agencies to prioritise the procurement of Australian-made cyber security solutions and services, providing Australian owned firms with a more secure market while fostering local innovation.

- **Prioritise Australian owned cyber security firms in procurement processes over international organisations:** It is imperative to give preference to local cyber security companies when making procurement decisions. The government can help these firms grow and become more competitive in the global market by leveraging the Australian Government as a customer or at least as an entity that has piloted a service or product.

- **Establish cyber security procurement guidelines for government agencies:** The government can create clear guidelines that outline the required security standards for products and services procured by public agencies, which can promote the adoption of best practices by Australian cyber security firms.

- **Promote public-private partnerships:** The government should promote public-private partnerships and joint ventures between local cyber security firms and international companies, providing Australian businesses with access to advanced technologies and global expertise. It is imperative that the process to select partnerships is transparent, accountable, and open to not disadvantage local Australian cyber security businesses.

- **Support research and development:** The government must invest in research and development initiatives aimed at advancing the cyber security sector in Australia, as well as offering tax incentives and grants to local firms that invest in cyber security R&D.

- **Encourage innovation through competitions and challenges:** The government can organise cyber security challenges and competitions to encourage local firms to develop innovative solutions, with winners potentially receiving procurement contracts or financial support.

- **International market access:** The government should expand support for Australian cyber security firms in expanding their presence in international markets by facilitating trade agreements, organising well-structured and planned trade missions.

- **Promote certification and standardisation:** The government should encourage Australian cyber security firms to adopt internationally recognised certifications and standards, enhancing their credibility and competitiveness in the global market.

- **Raise awareness of Australian owned cyber security firms:** The government should launch campaigns and initiatives to raise awareness about the capabilities of Australian owned cyber security firms, and the benefits of procuring locally developed solutions and services.

It is important to recognise the difference between wholly owned Australian cyber security firms or providers versus Australian cyber security firms or providers who are actually owned by foreign entities. Support should primarily be given to wholly owned Australian cyber security firms to prevent the exploitation of "Australian Made" which is actually "Foreign Entity" owned.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

The strategy should be reviewed regularly and updated frequently to incorporate emerging technologies, changing threat landscape, and evolving best practices. The national strategy document needs to be an active reference guide when making decisions and evaluating new technologies.

The government should leverage expertise of the industry, academia, and sector representative such as AISA to better understand the emerging technologies – both the risks and opportunities they bring in terms of the cyber security. It is important for the nation's strategy to adapt and evolve to keep up with the changing landscape and then accordingly review and update requirements for robust policies and procedures, advanced controls, compliance, and accountability to harness the risks and opportunities of the emerging technologies. It is fundamental to bring the government, industry, and community together to build a comprehensive and inclusive cyber security capability in Australia. By working together, these stakeholders can collaborate on developing effective policies and initiatives that address the challenges and opportunities presented by the rapidly evolving cyber security landscape.

Robust policies and regulations, designed on the understanding of the risks associated with emerging technologies, will assist with promoting concepts such as security by design by implementers, service, and platform providers. These policies and regulations will provide guardrails clearly connecting the purpose, requirements, and risks associated. Achieving cyber resilience requires a careful balance between regulations, innovation, and awareness. Regulations and standards can provide a necessary framework for promoting best practices and ensuring compliance, while innovation can drive the development of new technologies and approaches that enhance cyber security.

As per recommendations stated in response to question number 15, the Expert Advisory Board should be expanded to include individuals from diverse backgrounds and expert areas to understand the effects of emerging technologies and to better comprehend issues that could arise from the implementation of these new technologies within workplaces and communities.

20. How should government measure its impact in uplifting national cyber resilience?

Prior to the implementation of the cyber security strategy, the government should clearly define the metrics that will be used to measure the success or failure of the strategy. In measuring the strategy's impact in uplifting national cyber resilience, the Australian government should adopt a comprehensive and multi-faceted approach which includes a combination of qualitative and quantitative metrics to assess different aspects. Measurements should be taken before the start of the strategy implementation to act as a baseline from which to compare. It is important to also communicate clearly to the public and business community that some metrics may go in the other direction and are not necessarily a failure of the strategy. For example, raising awareness is likely to trigger a higher degree of incident reporting. This does not mean the strategy is not working as the data will begin to normalise over time. This normalisation period may take several years as more and more businesses and the general public become aware.

Suggested metrics and methods include:

- **Cyber Insurance:** Assess the adoption of cyber insurance policies among businesses in different sectors and use policies underwritten as an approximate proxy for the level of risk management and preparedness. Be careful not to get too caught up with this metric. The adoption of insurance across many sectors may not be a positive indicator and may simply indicate organisations electing to transfer risk as opposed to investing to remove or reduce the risk. Quantitative measure.

- **Supply Chain Security:** Evaluate the effectiveness of measures taken across critical infrastructure sectors to secure supply chains against cyber threats, including the implementation of cyber security standards (e.g. ISO27000 series) and best practices among suppliers. Quantitative and qualitative measures.

- **Public-Private Partnerships:** Measure the quantity and level of success of public-private partnerships in addressing cyber resilience challenges, sharing resources, expertise and information. Measuring the number and frequency of sector specific collaborations and peer sessions as a proxy for information sharing. Assess which sectors do not conduct this type of peer sharing and the maturity of the sharing (e.g. ad hoc, infrequent, regular etc). Quantitative and qualitative measures.

- **Cross-Sector Collaboration:** Measure the degree of collaboration and cooperation between government agencies, private sector organisations, and international partners in enhancing national cyber resilience and protection of consumer data. Quantitative measure.

- **Adoption of Cyber Security Frameworks:** Assess the level, maturity of adoption and implementation of cyber security best practices, standards and frameworks by public and private sector organisations. This can include the Australian Cyber Security Centre (ACSC) Essential Eight, NIST Cyber Security Framework, ISO/IEC 27000 series. Include privacy standards such as AS27701:2022. Assess which sectors are more mature versus immature to assess if there are changes in maturity over time. Quantitative measure.

- **Cyber Security Investment:** Analyse the allocation of resources, including financial investments and research and development funding dedicated to enhancing national cyber resilience. Perform state by state comparison and produce a national view. Consider also producing a sector-by-sector view of cyber security investment (e.g. operational baseline and future planned investment in technology, processes and people). Quantitative measure.

- **Workforce Development:** Evaluate the availability and skill level of cyber security professionals in Australia. This can be measured by the number of professionals employed / looking for employment, the number of graduates from cyber security programmes produced each year and how many gain meaningful employment in the sector, and the availability of cyber security training initiatives. In addition, the number of graduate / intern placements created / vacant can be included in the assessment. Quantitative measure.

- **International Benchmarking:** Compare Australia's cyber resilience performance against international benchmarks and best practices with countries in Europe and AUKUS. This can involve comparing cyber security rankings, such as the Global Cyber Security Index, performing a Cyber Security Capacity Maturity Model for Nations (CMM delivered by OCSC), and participating in international exercises, like the Cyber Defence Exercise. Quantitative measure.

- **Incident Metrics:** Track the number, type, and severity of cyber incidents experienced by government agencies, businesses, and individuals in Australia. This data can help assess the overall effectiveness of resilience measures and identify areas for improvement. Data can also indicate the level of preparedness across the nation. Expect the number and type of cyber incidents to initially increase as businesses and consumers become more aware of cyber issues and where to report them. Some data already exists such as information collected by ACSC, IDCare, ACCC (Scamwatch) and NDB reporting. Quantitative measure
.

- **Recovery Time:** Assess the average time taken to recover from a cyber incident across different sectors, including the restoration of systems, data, and operations. Faster recovery times indicate a higher level of resilience in those sectors. Quantitative measure.

- **Threat Intelligence Sharing:** Evaluate the effectiveness and timeliness of threat intelligence sharing between government agencies, private sector organisations, and international partners. This can be measured by the speed of information dissemination and the number of actionable intelligence reports shared. For example, the private sector is faster and more efficient than the ACSC in reporting threats to businesses. Quantitative measure.

- **Resilience Testing and Exercises:** Assess the frequency and effectiveness of resilience testing and exercises conducted by government agencies and critical infrastructure organisations. This can help identify vulnerabilities and areas for improvement across sectors. Quantitative measure.

- **Legislative and Regulatory Compliance:** Evaluate the effectiveness and enforcement of relevant cyber security laws, regulations, and guidelines. Quantitative measure.

- **Public Awareness and Education:** Measure the reach and effectiveness of cyber resilience awareness and behavioural change campaigns targeting the general public and specific groups such as small and medium-sized enterprises. Assessments can be done through surveys and assessments of cyber security knowledge and practices by working with organisations who help support these groups. For example NAB / CBA / ANZ / Westpac for banking customers (business and personal), CPA Australia (Accountants and their customers) and PEXA (lawyers, conveyancers and 160+ financial institutions). AISA can assist with surveys across cyber security professionals. Quantitative and qualitative measures.

21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

To support ongoing public transparency and input regarding the implementation of the cyber security strategy, it is essential to establish evaluation measures that are clear, comprehensive, accessible, collaborative and measurable. It is imperative the government considers the following evaluation measures:

- **Quarterly Public Reporting:** Publish quarterly reports on the implementation progress of the cyber security strategy. Published reports should detail the objectives, milestones, challenges faced, and successes achieved against the various pillars of the strategy. These reports should be made publicly accessible to promote transparency.

- **Public Consultations:** Continue to organise public consultations, workshops, and town halls to gather input and feedback from diverse stakeholders, including individuals, businesses, academia, and non-governmental organisations on a six-monthly basis to track the perception of progress, address any changes or to enlist engagement from businesses to assist in the strategy as it progresses over time.

- **Stakeholder Engagement:** Encourage collaboration and information-sharing between public and private sector stakeholders through joint initiatives, public-private partnerships, and the establishment of cross-sector working groups which meet quarterly to every six months.

- **Multi-stakeholder Approach:** Foster a multi-stakeholder approach, including civil society, academia, and the private sector, to promote transparency, inclusiveness, and public input in the development and implementation of the cyber security strategy as it progresses each year.

- **Independent Audits:** Conduct independent audits of the cyber security strategy and its implementation to ensure the accountability of responsible agencies, organisations and other stakeholders. The audit results should be made public to foster trust and build transparency.

- **Open Data:** Promote transparency by making relevant data and statistics on cyber security incidents, trends, and best practices publicly available.

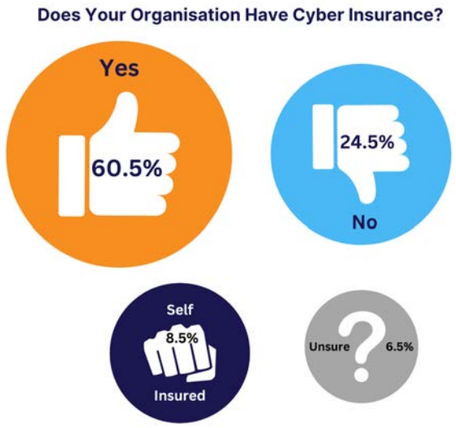
Cyber Security Insurance

Discussions at townhalls and roundtables regarding cyber security insurance were very contentious with most leaders in the sector raising a perception that cyber insurance was difficult to obtain, too few actual providers of the insurance, the premiums were very high with a reduction in actual coverage compared to previous years. When executives and CISO / CSOs were asked if their organisation had cyber insurance, 60.5% responded that they had some form of cyber coverage.

When asked if their cyber insurance provided value for money, 23.8% of Executives and CISOs responded that it did provide value, 46.6% stated "No" and 29.5% were unsure.

Across the entire market of those who had cyber security insurance, 25.5% believe it provided value for money, 32.8% believed there was no value and 41.7% were unsure.

When asked about the type of insurance coverage organisation have, Executives and CISO/CSO responded with the following:

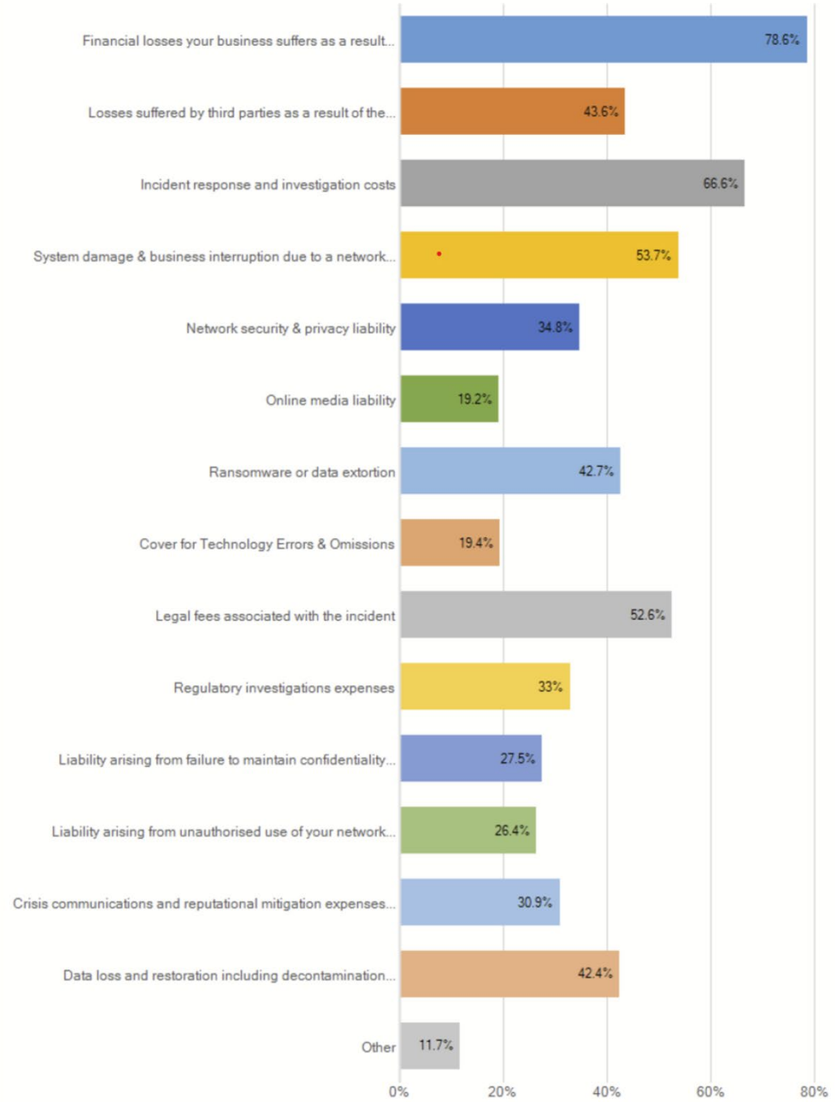


The five highest rated coverage areas for cyber insurance in order are:

1. Financial losses your business suffers as a result of a cyber incident (known as first party cover)
2. Incident response and investigation costs
3. System damage & business interruption due to a network security failure or attack, human errors, or programming errors
4. Legal fees associated with the incident
5. Losses suffered by third parties as a result of the incident (known as third party cover)

Based on data collected by AISA, most CISO / CSOs and Executives report the primary reason their organisation has cyber insurance is for contractual requirements to do business with other businesses. A secondary and less preferred reason to have cyber insurance is to align cyber security risk to match organisational appetite.

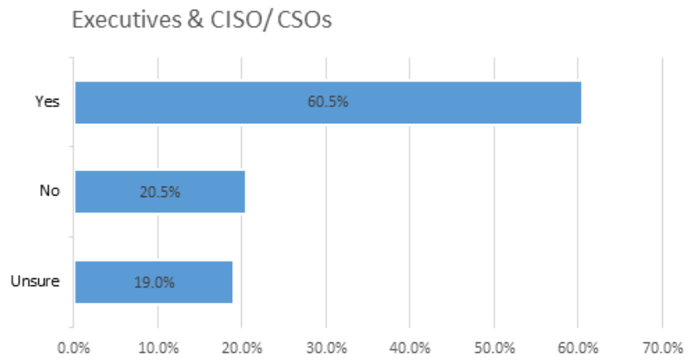
Types of insurance cover

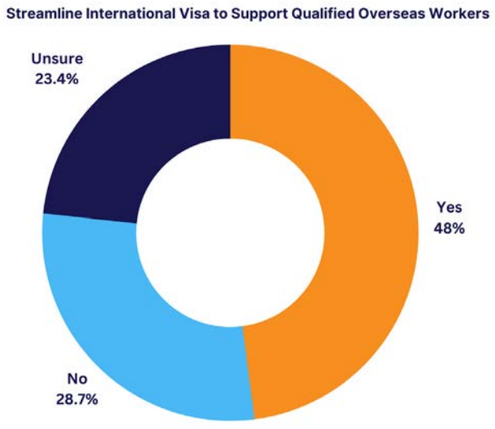


Role immigration changes could play to assist Australia with current cyber security challenges

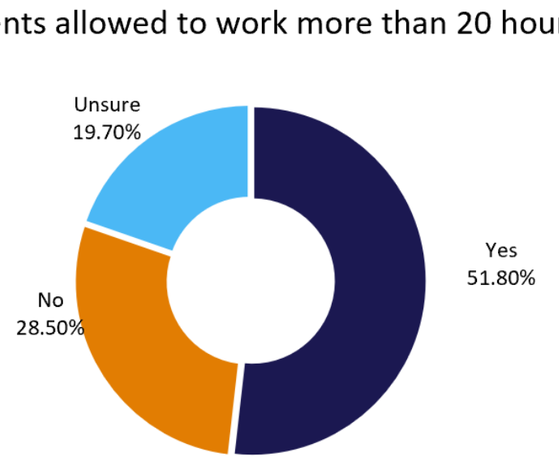
We asked the cyber security sector their opinion on how immigration changes could help address some of the cyber security challenges Australia is facing currently.

48.0% within the sector are in favour of the government streamlining the international Visa system to facilitate brining in more qualified workers within the sector from overseas. However, it's important to note that there are also 28.7% who are not in favour of this idea or 23.4% who are undecided. Further analysis based on personas suggests that senior leaders and executives in the sector are more likely to support this approach – 60.5% said 'Yes'.

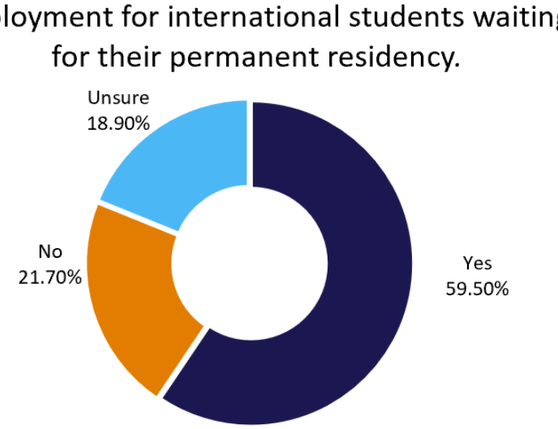




The survey asked if the government should consider allowing international students who are studying cyber security in Australia, to work more than 20 hours within the sector – 51.8% responded to be in favour, with 28.5% against the suggestion and 19.7% are undecided.



When asked if efforts should be made to encourage employment of international students, who have completed their cyber security course in Australia and are waiting for their permanent residency, 59.5% said 'Yes', with 21.7% saying 'No' and 18.9% were undecided. This aspect is important to ensure these students gain hands on experiences in the cyber security sector and the 20 hour limit on Visas does not act as an inhibitor. While Australia benefits from the revenue and capacity of international students, we need a working arrangement that promotes those individuals to work in cyber security as opposed to finding it difficult to get a role in cyber security and subsequently end up driving a taxi or working in the gig economy delivering food.



Skills, big picture view

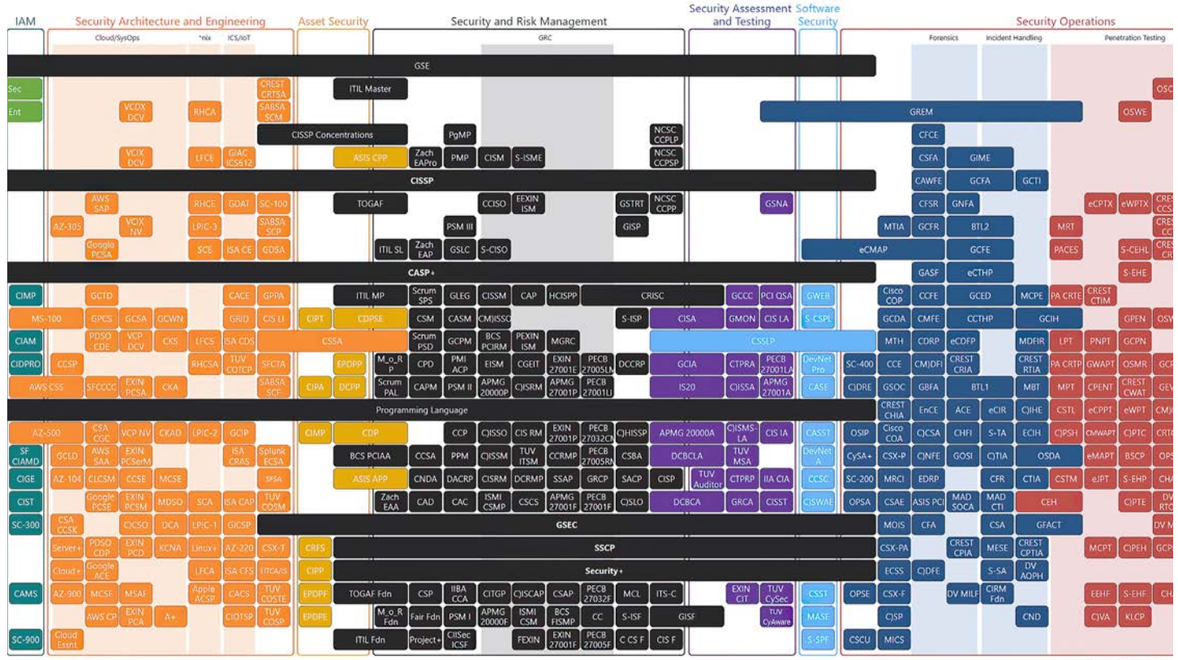
While AISA acknowledges a majority of people in cyber security today have entered via non-traditional pathways, this will not necessarily be the case in the future with the rapid increase of education providers and certification organisations. As of this report there are 473 global cyber security certifications. These certifications vary in quality and usefulness depending on an individual's job role function. Unfortunately, some of these certifications have become the de facto minimum benchmark for entry level jobs advertised on popular job sites. Frustratingly for graduates of traditional cyber security tertiary courses, these industry-based certifications often require five years of work experience, resulting in many graduates not applying for roles they could be qualified for. To break this cycle and provide hands on experience for graduates AISA proposed several options to Government in this submission. An out of the box thinking option is to create Cyber Defence Centres (CDC) in alignment with the JCSC, where tertiary providers (University / TAFEs) could place students for 3 to 6 month apprenticeships as part of their courses.

These national CDCs could provide services back to the community under the guidance of the ACSC / JCSC and industry in partnership. Services could be defined as:

- Cyber security health checks for SMEs.
- Cyber security advisory for businesses.
- Basic penetration / vulnerability testing and reporting services.
- Cyber security awareness and culture training.
- Basic SOC services.
- Basic consulting services.

These basic services do not take business away from existing consultancy, integrators and managed service providers as many SMEs would not be able to afford their services. However, a student run industry-based partnership model, would help produce students with hands on experience that these providers may want to employ at the completion of the student's study. In addition, these SMEs gain improvements in cyber resilience at minimal cost. If the SMEs want a higher level of service or offering, they could then be moved or referred to commercial consultancy, integrators and managed service providers, thereby expanding the market for these services.

The model can become self-sustaining with students training the next cohort of students, Universities/TAFEs could improve the system by tailoring their offerings to ensure students are ready for their CDC placement and industry experts could volunteer their time and services to coach and mentor students. For example, NAB employees often have to do 2 days a year of community service. Rather than NAB's 300+ security staff packing boxes in a warehouse, they could each contribute 2 days to the CDC. This alone would equate to 600 days of skilled resources to contribute to a CDC. CBA have a larger number of cyber security staff and could contribute in a similar way. CISO/CSOs who are retiring could also give back and volunteer their time to help the next generation of skilled workers.



Source: Paul Jerimy (https://pauljerimy.com)

People

Lead Authors

Akash Mittal

Board Director, AISA

Damien Manuel

Chairperson, AISA

Alex Hoffmann

Deputy Chair, AISA

Contributing Authors

Emily Wingard

Branch Chair, SA AISA

Raul Pascu

Deputy Chair, WA AISA

Craig Ford

Board Director, AISA

Contributing Authors

EJ Wise

Fellow & EABC, AISA

Nigel Hedges

Fellow & EABC, AISA

Ben Doyle

EABC, AISA

Joshua Craig

Board Director, AISA

Megan Spielvogel

General Manager, AISA

About AISA

The Australian Information Security Association (AISA) is both the peak body, and the largest organisation representing cyber security practitioners in Australia. AISA has over 10,500 members and corporate partners and is committed to the development of a robust information security sector through building the capacity of professionals, advancing the cyber security and safety of the Australian public as well as businesses and governments.

AISA's foundation scholarship fund will provide scholarships to build a career in cyber security by supporting education for women, rural and regional youth, Aboriginal and Torres Straight Islanders and those from disadvantaged backgrounds. The foundation has been fully endorsed as a deductible gift recipient (DGR).

Australian Information Security Association

Australian Information Security Association (AISA)
ABN 181 719 35 959
Level 8, 65 York Street, Sydney NSW 2000
(02) 8076 6012
info@aisa.org.au | www.aisa.org.au