WorkVentures
social inclusion through technology

Australian Cyber Security Strategy

2023-2030

Horizon II

Public Discussion Paper Submission

About WorkVentures

WorkVentures is Australia's leading IT social enterprise. As a not-for-profit, we are focused on transforming Australia through technology, skills and meaningful career pathways. We work with business, government and the for-purpose sector to bridge the digital divide, provide equitable career pathway opportunities and promote a circular economy. We deliver a range of cyber security solutions tailored to the NFP sector and a cyber career pathway program to increase diversity and skills within the sector and broader industry.

We welcome the opportunity to contribute towards shaping Horizon 2 of the Australian Cyber Security Strategy and building on progress generated from many of the Horizon 1 initiatives implemented by government.

> WorkVentures have helped to secure and create awareness amongst approximately 400 NFP organisations and protected the data of hundreds of thousands of vulnerable people across Australia.

This positions us strongly to provide recommendations on 'shield 1: strong business and citizens', particularly around the unique challenges faced by NFPs and solutions that can be implemented to build proportionate safeguards and resilience across the sector.

Additionally, 'shield 5: sovereign capabilities', aligns with WorkVentures' cyber cadetship programs that aim to build diversity within the Australian cyber workforce. WorkVentures supports the government's existing efforts in attracting global talent through migration reform, including the introduction of new skilled migrant visa categories, the MATES scheme and National Innovation visa.

We believe that cadetship programs also have a strong part to play in unlocking unrealised potential domestically and establishing strong sovereign cyber capability, as demonstrated through our most recent programs.

1 Strong businesses and citizens

Q8.

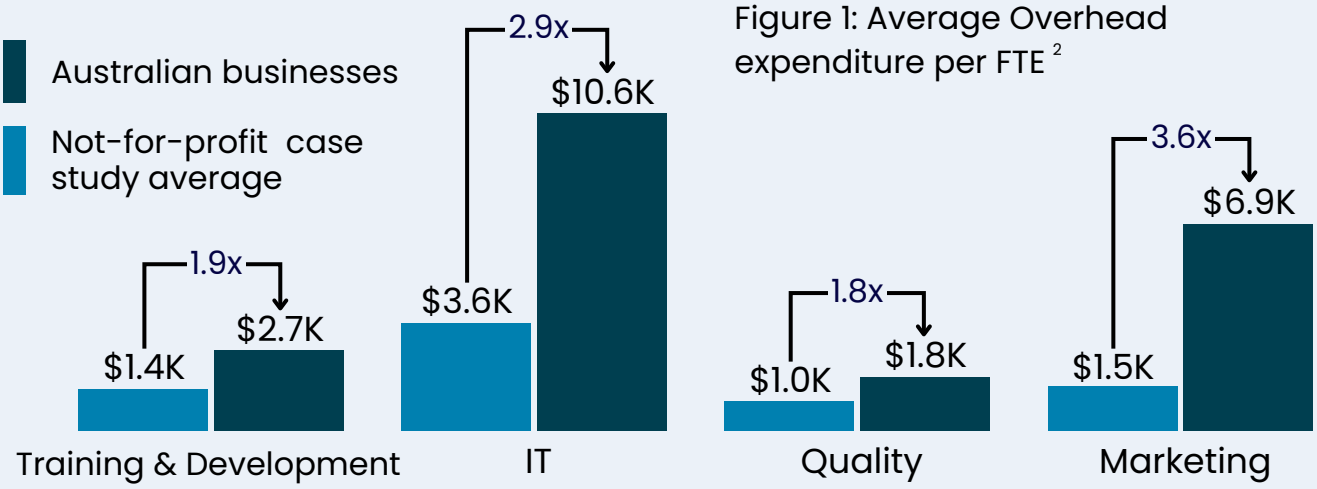
How can industry at all levels and government work together to drive the uptake of cyber security actions by SMEs and the NFP sector to enhance our national cyber resilience?

Time and resources are currently the biggest roadblocks preventing not-for-profit organisations from building a greater degree of cyber readiness and resilience. Many of these organisations are constrained by tight internal budgets that allow for very little spending on anything outside of the direct delivery of their programs and services.[1] With a shortfall in overhead funding of 13-23% for most grants, NFPs do not have sufficient capacity to allocate funding to securing the data that is processed and stored under their programs. This makes implementing effective cyber security controls difficult for NFPs who receive a high percentage of their total revenue from government funding.

Nearly 400 NFPs are entirely funded by government, with 7500 organisations generating more than 50% of their income from government funding.

There is **$107 billion** worth of government funding put into the charity sector, with nearly **$11 billion** of this being managed by relatively small organisations who operate on less than **$10 million** per annum. Our analysis has determined that organisations of this size face disproportionate cyber risk exposure.

Figure 1: Average Overhead expenditure per FTE [2]



For every dollar an Australian business spends on IT and cyber security per employee, a charity spends just 34 cents.

This stems largely from constraints in grant criteria around funding indirect costs, which if properly funded would allow for a more effective and impactful execution of their mission.[3]

1 Typical NFP indirect costs are c.33% of total expenditure while overhead funded by grants is only 10-20%: Social Ventures Australia, Centre for Social Impact & Philanthropy Australia 2022, Paying What it Takes: Funding Indirect Costs to Create Long-Term Impact, Social Ventures Australia, Sydney. https://www.socialventures.org.au/our-impact/paying-what-it-takes-report/

2 Mercer Human Resource Effectiveness Monitor, 2015 (adjusted for inflation to 2020 dollars), 2020 Infoxchange, https://www.infoxchange.org/au/digital-technology-not-for-profit-sector.

3 R Wilkie, J Edwards and L Goldstone, 'Future proofing: automation and outsourcing opportunities', PricewaterhouseCoopers (PwC) website,

Q8. *continued*

How can industry at all levels and government work together to drive the uptake of cyber security actions by SMEs and the NFP sector to enhance our national cyber resilience?

Case Study

WorkVentures performed a cyber risk assessment for a First Nations organisation who provides social housing and disability services, funded by their peak body. This organisation receives nearly half of their total revenue from government grants and were unable to fund the services internally. WorkVentures worked alongside the organisation to provide a full breakdown of their key cyber risks and a strategy to remediating these findings.

The organisation had taken this implementation plan to their senior management, but before they could find resources to putting this plan into place, a key vulnerability identified within our assessment was successfully exploited by a threat actor who was able to gain unauthorised access to their environment and large volumes of sensitive data. This had a considerable impact on short-term operational continuity and financial loss because of the need to engage emergency resources to support incident response and recovery.

As represented through the case study above, this is a very real problem for the sector. A solution to this is to build provisions into existing grant funding that allow a percentage to be allocated towards cyber security services to help organisations meet a baseline level of controls. To gain a level of assurance that this baseline has been effectively implemented prior to awarding a contract, NFPs should be independently certified against an industry standard, such as SMB1001, with the grant funding allocation to uplift this to the baseline within the period of the grant term. This would help to secure continuity of services for over $107 billion of government funding and prevent the sensitive and personal information of our most vulnerable communities from falling into the wrong hands.

With our singular focus upon the NFP sector, WorkVentures Cyber is uniquely placed to support government with these assessments and uplifts for the NFP sector. While broader uptake of existing government initiatives, including the Small Business Cyber Resilience Service and Cyber Wardens, will certainly support NFP uplift, they do not consider the unique challenges and threats facing the NFP sector (refer Q10). Nonetheless these programs can be complimentary as part of the SMB 1001 certification, NFPs could be recommended to enrol in the Cyber Wardens program or implement a process to refer to the Small Business Cyber Resilience service to meet requirements within the standard.

Q9.

What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFPs?

[redacted]

to comply with such standards are in many cases driven by commercial needs to comply with clients' information security requirements, that often do not exist within the small-medium sized NFP sector. Whilst Essential 8 provides a much more straightforward and prescriptive approach to implementing a cyber security program within an organisation, it does not provide holistic coverage against the plethora of vulnerabilities that are being actively exploited by threat actors and so may leave NFP's exposed.

To best service the needs of Australian NFPs, a reliance on holistic standards and frameworks, such as the **Centre for Internet Security's (CIS) Implementation Guide for Small and Medium Sized Enterprises framework**,

[redacted]

an effective strategy in place that also considers aspects of information security such as governance, resilience and awareness, that are key to mitigating prevalent threats.

SMB1001 works well alongside our recommendations under question 8, as it allows organisations to be independently certified against the standard to provide government, beneficiaries and partners with a level of assurance that the organisation meets a baseline level of controls. This also brings a level of enforceable accountability to NFP organisations regarding their cyber security posture, where currently there are little to no benefits for these organisations to invest in securing their data from a commercial perspective.

Q10.

What are the unique challenges that NFP entities face for cyber security compared to the broader business sector and what interventions from government would have the most impact in the NFP sector?

NFPs are uniquely challenged as they store and process sensitive data on behalf of our most vulnerable communities but also have considerable resourcing and funding constraints that make securing this data incredibly difficult. A higher dependence on volunteers and part-time or casual staff means that despite the size of each organisation, they commonly have a larger number of total employees because of the nature of their workforce. This introduces challenges from an IT perspective, particularly when it comes to procuring company managed devices which have a standard operating environment with basic controls such as centralised authentication, configuration and patch management, as well as endpoint protection, full-disk encryption and narrow user permissions. This means that NFPs are subject to greater risk of data exposure or loss because of organisational data being accessed from and stored on devices with minimal controls in place to lower the risk of compromise.

The workforce factor does not only pose challenges from a technical perspective, but also when it comes to ensuring that staff have an adequate level of awareness against human-centric threats like phishing and other forms of social engineering. The reliance on volunteers, as well as part-time and casual staff, means that staff are onboarded and offboarded from NFP organisations very frequently and staff retention is a growing challenge.[4] This often results in difficulties in building up the sectors overall level of security awareness and a higher likelihood of falling victim to threats including ransomware, business email compromise and credential harvesting, leading to financial loss and unauthorised access to systems. This risk is heightened when considering that the NFP sector has a relatively higher level of cultural and linguistic diversity, resulting in a greater inherent risk to phishing.[5]

The challenge for NFPs is increasingly complex, not only because threats are more prevalent and damaging to organisations but also because the controls that are necessary to limiting risk exposure are becoming more expensive. Microsoft's offer for Australian NFPs to procure free Business Premium licenses, meant that organisations within our sector were able to access enterprise grade security and device management features without spending on paid licenses.

4 Australian Council of Social Service. 'At the precipice: Australia's community sector through the cost of living crisis', At the precipice: Australia's community sector through the cost of living crisis - ACOSS.

5 National Anti-Scam Centre. 'Targeting scams: report of the National Anti-Scam Centre on scams data and activity 2024'.

Q10. *continued*

What are the unique challenges that NFP entities face for cyber security compared to the broader business sector and what interventions from government would have the most impact in the NFP sector?

With this grant lapsing in July 2025, we have seen organisations moving to free **Business Basic licenses which lack the foundational controls required to adequately protect the organisation's data**, including endpoint detection, device and mobile application management, conditional access policies, encryption and various other foundational controls.

Interventions from government that would have the most impact in the sector are proactive initiatives to strengthen the cyber readiness of NFPs, rather than just focusing on resilience. This includes initiatives like those detailed in our question 8 response, as well as funding to identify and manage key cyber risks within the highest risk cohort of NFP organisations. This cohort is made up of organisations storing and processing highly sensitive data such as personally identifiable information and those whose funding comes largely from government grant programs.

A cyber incident or data breach within this group of organisations would have a significant financial, operational and reputational impact, as well as a direct, and potentially life-threatening impact on the vulnerable people that they serve, and a risk to the continuity and fulfilment of government-funded programs. Committing a minimum provision for cyber security spend of $25,000 for grants under $5 million and 0.5% of the total grant funding for grants above $5 million will provide significant risk reduction for the sector and contribute towards protecting the data of millions of vulnerable Australians. If this was applied to the entire population of NFPs who receive grant funding, this is estimated to cost less than 1% of government's total investment in the charity sector. By taking a risk-based approach and focusing on the organisations that process and store the most sensitive data, such as those within the domestic and family violence sub-sector, this would be a cost effective and impactful approach to securing not-for-profits.

In addition to creating provisions for cyber security spend within grant funding, we also see a role for the Australian government to play in collaborating with leading technology providers such as Microsoft, to ensure that licenses giving NFPs access to enterprise-grade security controls are made accessible once more. This is achievable through a range of methods, including but not limited to public-private partnerships with major technology providers, dedicated grants or by recognising vendor contributions to the sector via digital philanthropy tax offsets.

affordable cyber security controls can be sought through government partnerships with big tech, grant funding and digital philanthropy tax offsets

Q14.

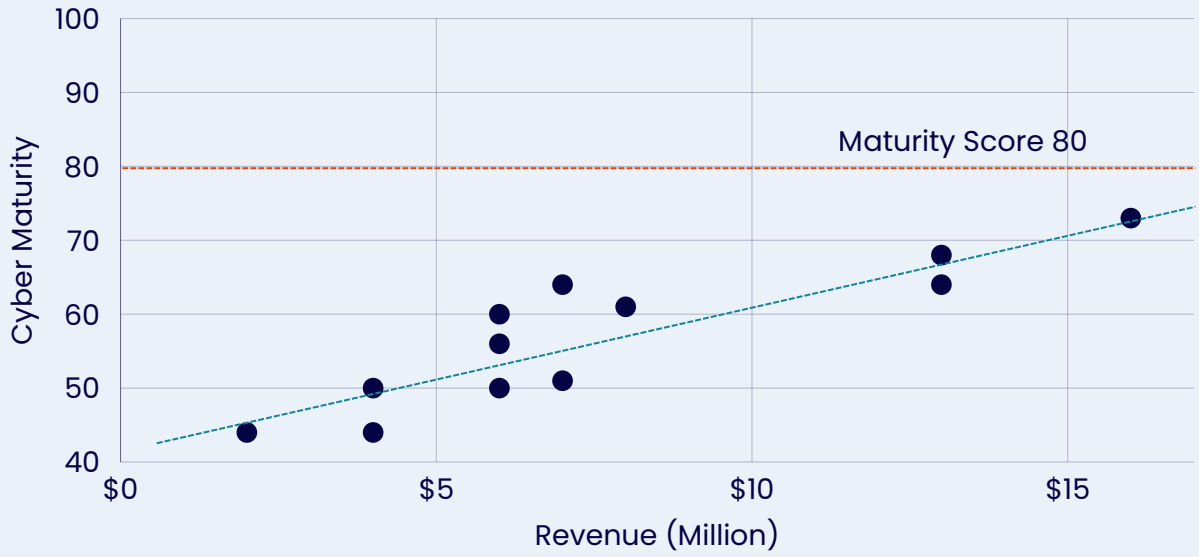
Have you experienced or researched any vulnerabilities or impacts from cyber security incidents that disproportionately impact your community, cohort or sector? If so, what were the vulnerabilities and impacts that your community faced?

In addition to our work in assessing and managing cyber security risk across the NFP sector, WorkVentures has recently undertaken a targeted program of work to assess the cyber security of NSW Social Service organisations in partnership with the peak body, NSW Council of Social Services (NCOSS).[6] This study demonstrated several areas of concern, as well as recommendations for NFPs and government to help support scaling cyber uplift across the sector.

At a high level, the findings are:

- Low cyber maturity
- Overreliance on external cyber management
- Lack of basic security measures

Relationship between revenue and cyber maturity



Cyber maturity is alarmingly low across the group that we assessed, with there being a direct correlation between the size of the organisation and their cyber security maturity.

This relationship is particularly concerning when we extrapolate our data out to the rest of the sector, as we know that 74% of charities have an annual revenue of less than $500,000; a quarter of the size of the smallest NFPs within our assessment.[7]

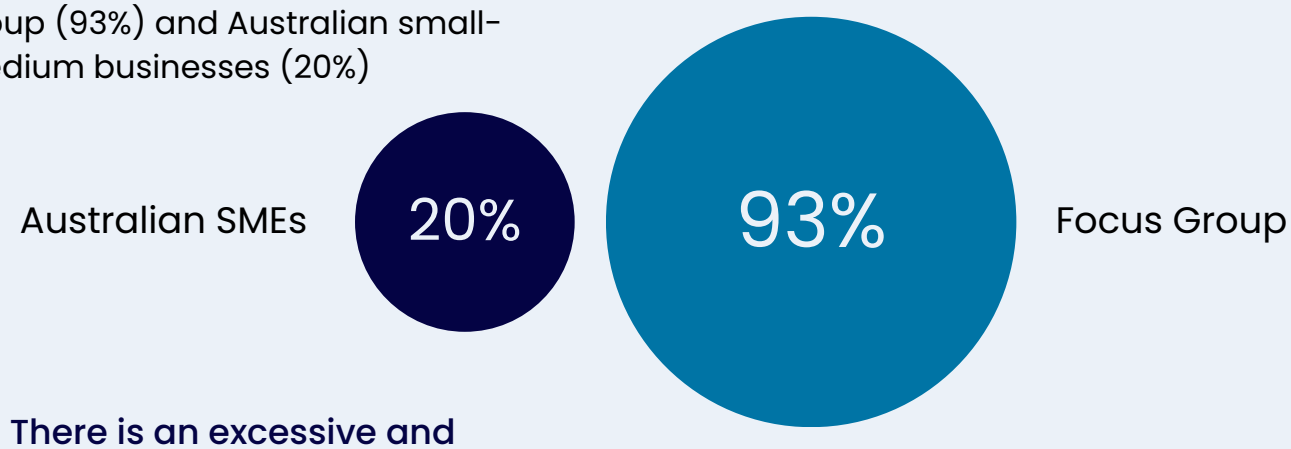
6 WorkVentures. 'Hidden Vulnerabilities: Cyber Security and Essential Community Services in NSW', Hidden Vulnerabilities: Cyber Security and Essential Community Services in NSW.

7 Australian Charities and Not-for-profits Commission. Australian Charities Report 11th edition, Australian Charities Report 11th edition, p. 13.

Q14. *continued*

Have you experienced or researched any vulnerabilities or impacts from cyber security incidents that disproportionately impact your community, cohort or sector? If so, what were the vulnerabilities and impacts that your community faced?

Figure 3: Spread of cyber insurance policy holders across the focus group (93%) and Australian small-medium businesses (20%)



There is an excessive and misplaced reliance on external parties to manage cyber security on behalf of the organisation.

This includes a trend of organisations transferring significant risks into cyber insurance instead of undertaking any internal activities to mitigate or avoid risk. In the case of one organisation who held a cyber insurance policy, they suffered a data breach as a result of not enforcing multifactor authentication across all Microsoft Office 365 accounts and falling victim to a credential harvesting phishing attack. This breach resulted in the disclosure of client personally identifiable information. This is not only concerning from a sector risk management perspective, but it also raises concerns around the barrier to entry for cyber insurance, as today, multifactor authentication is widely considered as table stakes.

Secondly, many NFPs are reliant on IT managed service providers to secure critical data and ensure system availability, however there are very few organisations who have conducted an independent assessment of their network and systems environment. WorkVentures polling across nearly 300 not-for-profit organisations has demonstrated that 70% have not conducted a recent and independent cyber risk assessment.

Lastly, NFP cloud migration has resulted in an increasing reliance on software vendors to effectively secure data. This has signalled an increase in third-party data breaches within the sector and underscores the importance of enabling access to expertise that can undertake effective third-party risk management activities.

Q14. *continued*

Have you experienced or researched any vulnerabilities or impacts from cyber security incidents that disproportionately impact your community, cohort or sector? If so, what were the vulnerabilities and impacts that your community faced?

Most organisations have not addressed the basics.

Despite the cost effectiveness and ease of implementation of many basic processes and controls that lower the impact and likelihood of compromise, organisations still cite resource constraints as their key challenge to building cyber readiness.

This issue is especially pronounced within the NFP sector due to limited internal expertise and lack of funds to engage external consultants.

Although this program of work was based on organisations in NSW, the selection of participating NFPs was intentionally designed to provide us with a broad range of organisations that exist within the sector from a revenue, service and employee headcount perspective.

Additionally, our cyber security services have allowed us to assist organisations right across the country and the results of this work show very similar trends to what was uncovered as a part of the NCOSS project. If we extrapolate the data out nationally, it paints a very concerning image of the sector's cyber security posture. Based on the trend between cyber security maturity score and revenue, as well as those that process and store highly sensitive data and are between 75-100% government funded, **WorkVentures estimates 1000 charities are at critical risk of a data breach.**

5
Sovereign capabilities

Q39.

What role should government play in supporting the development and growth of Australia's cyber workforce? What initiatives, pilots or policy ideas do you think would best support industry to grow?

The government's aim to become a world leader in cyber security by 2030 is only achievable through the support, development and growth of our cyber workforce. Part of this also comes down to supporting small and medium businesses to strengthen their cyber security posture. Funding is critical and cyber education and training is essential, especially considering the sensitivity of the data that the sector is storing and processing on behalf of the people they support. As demonstrated in the responses above, the impact of a data breach is substantial.

Consistent breaches in the NFP sector would erode the confidence that society places in organisations as providers of quality and trusted services to people living in poverty and disadvantage, requiring financial outlay from the government in other ways.

When we launched our federally funded (Dept of Industry) Cyber Cadetship program, the results reinforced what we knew to be the case; there was an untapped talent source that simply required some additional, direct training and development. Once this was attained, we saw the participants flourish and move into corporate and government roles.

With over 1000 applicants to our program, through renewed funding, replication and scaling, we know we can have a wider impact.

Government can play a direct role in funding programs that build a pipeline of skilled and diverse cyber security professionals for industry and government, whilst simultaneously helping to secure the data of our most vulnerable Australians. Cadetship programs provide early career professionals, as well as those in mid-career transitions with the experience that helps them link academic knowledge to real-world problems and solutions that can be applied to secure different parts of the Australian economy. Shared funding models between industry and government, whereby funders can secure a pipeline of talent by contributing towards the investment into cyber cadetship programs, can also help to solve industry problems around unrealistic hiring criteria and an unclear pathway into the profession.

WorkVentures estimate a cost of of between $30-$40,000 per cadet to go through a 6-month cadetship program and upskill prior to entering a public sector or corporate role. This cost could be shared between government and industry partners to incentivise investment into early career professionals forming a cyber skills pipeline. By providing payment through the cadetship, it enables people from diverse backgrounds to apply, thus increasing the candidate pool.

Q40.

What have been the most successful initiatives and programs that support mid-career transitions into the cyber workforce and greater diversity in technology or STEM-fields more broadly?

WorkVentures' cyber cadetship programs have contributed to building a skilled and diverse cyber workforce, as well as sovereign capability in the cyber domain, seeing **100% of participants progress into full-time employment and 40% move into government cyber roles.**

This program has helped develop and nurture skills and knowledge within diverse cohorts that were being overlooked by industry and government talent acquisition processes. Our program enabled skill development whilst contributing to the cyber readiness and resilience of the NFP sector.

The program was broken down into a 3-stage career accelerator, focused on creating alternative pathways into the industry for people from diverse backgrounds. The high quality of the participants, the level of their education, and the commitment they displayed was inspiring and confirmed our thoughts, that for some time we have observed diverse, skilled workers struggling to secure work in Australia. Our accelerator programs uncovered groups of candidates with excellent skillsets and the drive to achieve.

Our program provided an environment in which participants:

- Developed professional skills, including teamwork, leadership, time management, and communication
- Honed their knowledge by working closely with internal and external cyber security professionals
- Utilised their unique skillsets to help protect the data of NFP's and vulnerable communities
- Were tested from both a technical and non-technical perspective

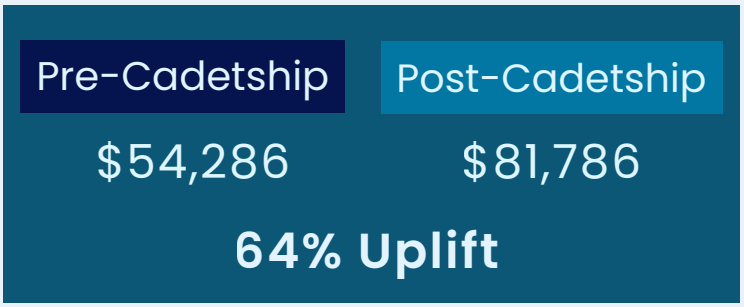


Figure 4: Average salary growth experienced from past cadet cohorts

Many who went through the program had a high level of education, with some holding a postgraduate level of education in information technology and cyber security, and others with previous experience working in the field. Most of these individuals had failed to break into the industry because they lacked local experience; others had been overlooked throughout standard hiring processes due to not 'ticking the boxes' of corporate talent acquisition.

When considering the government's cyber workforce objectives under Horizon 2, cyber cadetship programs are a proven method of supporting both mid-career transitions and groups of diverse individuals into careers in the cyber security industry. This is also true for STEM-fields more broadly, showcased by our Youth Employment Solutions team assisting more than 25,000 young people, with a strong focus on STEM.

WorkVentures
social inclusion through technology

[redacted]

[redacted]

Web: workventures.com.au